Software Engineering Institute

International Implementation of Best Practices for Mitigating Insider Threat: Analyses for India and Germany

Lori Flynn (Software Engineering Institute)
Carly Huth (Software Engineering Institute)
Palma Buttles-Valdez (Software Engineering Institute)
Michael Theis (Software Engineering Institute)
George Silowash (Software Engineering Institute)
Tracy Cassidy (Software Engineering Institute)
Travis Wright (Carnegie Mellon University,
Master of Science in Information Security Policy and Management Program)
Randy Trzeciak (Software Engineering Institute)

April 2014

TECHNICAL REPORT
CMU/SEI-2014-TR-008

CERT® Division

http://www.sei.cmu.edu

Carnegie Mellon University

Copyright 2013 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

This report was prepared for the
SEI Administrative Agent
AFLCMC/PZM
20 Schilling Circle, Bldg 1305, 3rd floor
Hanscom AFB, MA 01731-2125

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution except as restricted below.

Internal use:* Permission to reproduce this material and to prepare derivative works from this material for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

External use:* This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

* These restrictions do not apply to U.S. government entities.

Carnegie Mellon® and CERT® are registered marks of Carnegie Mellon University.

DM-0000801

Table of Contents

List of Figures

List of Tables

Acknowledgments

This work was funded by a generous grant from the Cyber Enterprise and Workforce Management directorate that is part of the CERT® Division at the Carnegie Mellon Software Engineering Institute. In addition to that directorate, we want to thank members of the CERT Enterprise Threat and Vulnerability Management team who provided helpful review comments and edits that enhanced this report, and improved its integrity: David Mundie, Mark Zajicek, and Andrew Moore. We give special thanks to our team members and SEI professional editors Pennie Walters and Hollen Barmer.

® CERT is a registered trademark owned by Carnegie Mellon University.

Executive Summary

This report applies a new framework for international cybersecurity analysis to specific countries for the first time. Using this framework, as outlined in the paper *Best Practices Against Insider Threats in All Nations,*[1] cybersecurity standards are considered with respect to a country's technologies, relevant laws, law enforcement, corruption, and prevalent culture and subcultures. That paper describes how these factors have major impacts on the effectiveness of implementing particular types of cybersecurity controls. Technical, physical, and administrative controls that are helpful for implementing cybersecurity best practices in India and Germany may be helpful for similar countries. Likewise, particular controls may be challenging to implement or be ineffective (and require substitution controls) in similar countries. In this report, we examine India and Germany, using cybersecurity best practices specific to insider threat mitigation for our analysis demonstration. First, we provide a detailed profile for each of these factors, for both countries. Next, we use the analysis framework to consider five best practices against insider threats recommended in the *Common Sense Guide to Mitigating Insider Threats*[2] (CSG). This report is intended to help organizations implementing cybersecurity best practices internationally, not limited to Germany or India, or to insider-threat-related cybersecurity. In part, this analysis is meant to help readers understand specific challenges in India and Germany, plus mitigations for the challenges that are particularly useful in those countries. These insights can be used by organizations that outsource to, offshore to, or have supply chains that include these countries. Furthermore, this report's analyses may be helpful on a wide scale for implementing cybersecurity best practices in countries with characteristics similar to those of India or Germany.

One reason why we chose Germany and India for this analysis is because they are major U.S. trading partners, and therefore, cybersecurity issues in these nations could significantly impact the United States. Beyond that, we selected those two countries for analysis due to their wide variation with respect to many factors, such as (a) their development status as a nation, (b) the sophistication of their communication networks and availability of the internet, (c) their reputation for the amount of regulation and degree of enforcement, (d) their reputation for corruption, and (e) the degree to which a national identity contributes to or impedes communication throughout the country. Findings in this report might be partially or fully reusable for countries with similar profiles, and, by choosing widely varying countries, our intention was to create findings applicable to many additional countries. Additionally, we considered the size of the population that would be analyzed, with a goal of including at least one highly populated country. India is the second most populated country in the world; analysis of India offers results that directly apply to 17% of the

[1] Flynn, L.; Huth, C.; Trzeciak, R.; & Buttles-Valdez, P. "Best Practices Against Insider Threats for All Nations." *Proceedings of the Third Worldwide Cybersecurity Summit*, New Delhi, India, Oct. 30-31, 2012. EWI and IEEE. Forthcoming. http://cybersummit2012.com/content/selected-papers

[2] Silowash, George; Cappelli, Dawn; Moore, Andrew; Trzeciak, Randall; Shimeall, Timothy; & Flynn, Lori. *Common Sense Guide to Mitigating Insider Threats*, 4th Edition (CMU/SEI-2012-TR-012). Software Engineering Institute, Carnegie Mellon University, 2012. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=34017

world's population.[3] Lastly, Germany exemplifies the complex nature of individual nations implementing European Union (EU) regulations, particularly with respect to data privacy concerns, so analysis of Germany was judged to be helpful for future considerations of other EU nations, many being major U.S. trade partners.

This analysis revealed important considerations that organizations should consider for their non-U.S. business partners, outsourcing, supply chains, and offshoring. The stated focus of the CSG is the United States. We found that some of the CSG's recommended controls would support best practices more effectively if modified or publicized differently for insider threat programs in (and covering) India and/or Germany. Additionally, we found some issues impeding effective implementation of some best practices, without yet finding an effective solution for them. This is an initial, exploratory effort that is not exhaustive.

This report contains the following information: the analytical purpose of and methodology used for this work; detailed profiles of India and Germany for each factor; analysis of issues related to effective implementation of five insider threat best practices in each country; a comparison of major select findings for each country; a summary of this report's findings; and a description of the future work planned.

[3] Although there are currently low rates of access to the internet in India, the analysis in this report can be used and updated in the near future when non-smartphones are expected to be replaced by widely affordable smartphones, resulting in high internet-access rates. And while the access rate was only 11% as of 2012—a seemingly low percentage—due to India's high population, that 11% still constitutes a large number of people with internet access.

Abstract

This report analyzes insider threat mitigation in India and Germany, using the new framework for international cybersecurity analysis described in the paper titled "Best Practices Against Insider Threats in All Nations," applying the framework to specific countries for the first time. Using that framework, cybersecurity standards are considered with respect to analysis that takes into account a country's technologies, relevant laws, law enforcement, corruption, and prevalent culture and subcultures. This report provides a detailed profile for each of these factors for each country and considers five best practices for mitigating insider threats recommended in the *Common Sense Guide to Mitigating Insider Threats.*

This report is intended to help organizations implement cybersecurity best practices internationally. In part, this analysis is meant to help readers understand challenges in India and Germany, plus mitigations for the challenges that are particularly useful in those countries. These insights can be used by organizations that outsource to, offshore to, or have supply chains that include these countries. Furthermore, this report's findings may be helpful on a wide scale for implementing general cybersecurity best practices in countries that share similarities with India or Germany, with regard to the factors studied. Technical, physical, and administrative controls that are helpful for implementing best practices in India and Germany may be helpful for similar countries. Likewise, particular controls may be ineffective (and require substitution controls) in similar countries. This is an initial, exploratory effort that is not exhaustive.

1 Introduction

This report applies a new framework for international cybersecurity analysis to specific countries for the first time. Using this framework, outlined in the Third Worldwide Cybersecurity Summit paper titled "Best Practices Against Insider Threats for All Nations" [Flynn 2012] cybersecurity standards are considered with respect to a country's technologies, relevant laws, law enforcement, corruption, and prevalent culture and subcultures. That paper describes how these factors have major impacts on the effectiveness of implementing particular types of cybersecurity controls. Technical, physical, and administrative controls that are helpful for implementing cybersecurity best practices in India and Germany may be helpful for similar countries. Likewise, particular controls may be challenging to implement or ineffective (and require substitution controls) in similar countries.

In this report, we examine India and Germany using cybersecurity best practices that are specific to insider threat mitigation. In Section 2, we provide a detailed profile of India and then examine how factors in the country affect implementation of five best practices for mitigating insider threats recommended in the *Common Sense Guide to Mitigating Insider Threats* [Silowash 2012]. We discuss each factor/best practice combination. In Section 3, we do the same type of analysis for Germany. Section 4 compares select major findings between the countries. In Section 5, we summarize the findings and describe our related work plans. The appendix contains summaries of the five cybersecurity best practices, including some U.S.-oriented implementation recommendations.

This report is intended to help organizations implementing cybersecurity best practices internationally, not limited to Germany or India, or to insider-threat-related cybersecurity. In part, this analysis is meant to help readers understand specific challenges in India and Germany, plus mitigations for the challenges that are particularly useful in those countries. These insights can be used by organizations that outsource to, offshore to, or have supply chains that include these countries. Furthermore, this report's analyses may be helpful for implementing cybersecurity best practices generally, in many countries with characteristics similar to those of India or Germany.

This report uses the definition of a *malicious insider* from the *Common Sense Guide to Mitigating Insider Threats* [Silowash 2010] written by the CERT® Division of the Carnegie Mellon Software Engineering Institute:

> *a current or former employee, contractor, or business partner who meets the following criteria:*
>
> - *has or had authorized access to an organization's network, system, or data*
> - *has intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems*

® CERT is a registered trademark owned by Carnegie Mellon University.

Throughout this report, the word *insider* is used only to signify *malicious* insiders; *unintentional* insiders are not addressed.

In part, we chose India and Germany for this analysis because they are major U.S. trading partners and thus, their cybersecurity issues might significantly impact the United States. Beyond that, we selected those two countries for analysis due to their wide variation with respect to many factors, such as (a) their development status as a nation, (b) the sophistication of their communication networks and availability of the internet, (c) their reputation for the amount of regulation and degree of enforcement, (d) their reputation for corruption, and (e) the degree to which a national identity contributes to or impedes communication throughout the country. See Table 1 for some of our considerations when choosing the countries. Findings in this report might be partially or fully reusable for countries with similar profiles, and, by choosing widely varying countries, our intention was to create findings applicable to many other countries. Additionally, we considered the size of the population that would be analyzed, with a goal of including at least one highly populated country. India is the second most populated country in the world; analysis of it offers results that directly apply to 17% of the world's population.[4] Lastly, Germany exemplifies the complex nature of individual nations implementing European Union (EU) regulations, particularly with respect to data privacy concerns, so analysis of Germany was judged to be helpful for future considerations of other EU nations, many of which are major U.S. trade partners. This is an initial, exploratory effort that is not exhaustive. For instance, on some topics, the resources we used had more information about one country than the other. Additionally, new revelations have appeared in the news during the writing of this report, and they affect analysis of technological systems (particularly with respect to encryption, monitoring, and storage of, and access to sensitive data) [Poitras 2013, Spiegel 2013d, Larson 2013]. These revelations also impact analysis of each country's laws, law enforcement, and culture, but, due to time constraints, we weren't able to consider all of them here.

The benefit of doing this analysis for multiple countries is the ability to compare and contrast the cybersecurity effects of differences between them, which would also be useful when considering additional countries beyond the scope of this report: Tentative extrapolation of similar issues for countries with similar profiles could be done, for instance, for countries with similar corruption and regulation profiles. This report can be used as a basis of data and analysis for further exploration of additional countries.

In addition to the considerations above, the CERT Division's sponsors have specified interest in research on these topics that our work addresses:

- combatting insider threats, noted as an important topic for further research by the U.S. Department of Defense (DoD) [Gabrielson 2008], U.S. Department of Homeland Security (DHS) [DHS 2012a], and Transportation Security Administration [DHS 2012b]
- the DoD's 2011 cyberspace "Strategic Initiative 4: Build robust relationships with U.S. allies and international partners to strengthen collective cybersecurity" [DOD 2011]

[4] Although there are currently low rates of access to the internet in India, the analysis in this report can be used and updated in the near future when non-smartphones are expected to be replaced by widely affordable smartphones, resulting in high internet-access rates. And while the access rate was only 11% as of 2012—a seemingly low percentage—due to India's high population, that 11% still constitutes a large number of people with internet access.

- external security dependencies including "cloud," identified by DHS as an important topic for future research [DHS 2012a]
- "supply chain," identified by the president of the United States [NSTC 2011] and the DoD [DOD 2012] as an important topic for further research

Table 1: Some Factors Considered for Country Choice

Factor	**India**	**Germany**
Trade with United States	$57.8 billion (15th biggest)	$147.5 billion (5th largest)
Highly developed		X
Developing	X	
Population	1.2 billion	82 million
Region		
Europe		X
Asia	X	
Latin America		
Africa		
North America		

The CERT Insider Threat Center works, in part, on internationally focused research, to help mitigate U.S. cybersecurity threats from (and to) the United States' international business partners, suppliers, allies, and adversaries. The CERT Division's previous research on international insider threat includes gathering case stories from foreign countries, although most of the division's cases and work focus on the United States. The CERT Division's other international insider threat work includes teaching computer security incident response team (CSIRT) and incident handling courses [cert.org 2013] that include some education about insider threats. For instance, individuals from a number of organizations in India and in other countries around the world have attended the CERT Fundamentals of Incident Handling (FIH) course[5]. This report's analysis of specific countries should help readers understand the context of the insider threat cases from those countries, as well as specific challenges and particularly useful mitigations that will inform the CERT Division's educational and consulting work in those and similar countries.

[5] The FIH course described at http://www.sei.cmu.edu/training/p26.cfm includes a session on insider threat.

2 India

2.1 Country Profile

In this section, we describe India in terms of five factors: information technology (IT) systems, relevant laws, corruption, law enforcement, and culture and subcultures.

India faces many interesting cybersecurity challenges and is encountering major changes to its cybersecurity profile that are related to both the unique ID [UIDAI 2013] nationwide rollout [Kumar 2013b] (which will provide a 12-digit unique ID to each citizen backed by biometric data, and has, since 2010, provided a unique ID for 350 million citizens [Kumar 2013b]) and the new affordability of smartphones for the poor that is expected soon. As of 2009, 83% of India's population was covered by a mobile network signal, and India has the fifth lowest cost per minute for mobile cellular calls of 142 nations compared in 2012 [World Economic Forum 2013]. This means that cellular communication access is both physically and economically feasible for many, including the poor. With smartphones, many will have their first access to the internet, and to banking, through their smartphone in rural areas. Many of these new users will be uninformed about cybersecurity practices and—due to a high rate of illiteracy in the rural areas and national and regional language barriers—may not be easily educated. (Only 62.8% of adults in India are literate [World Economic Forum 2013].) The government of India is interested in securing its critical infrastructure. For example, it recently took part in a two-day joint cybersecurity exercise between the United States's computer security incident response team (US-CERT) and CERT-In (CERT India) [Kumar 2012]. Working on India's major cybersecurity challenges also offers opportunities to make a huge impact by helping the 1.2 billion people who live there—17% of the world's total population. India is the 15th biggest trading partner for the United States with $57.8 billion annually in exports and imports between the two, and is a major U.S. supplier of outsourced software engineering. The cultural landscape of India is heterogeneous, with strong regional cultures and identities that are often linked to language affiliations. For example, approximately 200 languages are spoken within the country, 22 of which are recognized as official languages. Below, we detail India's technological profile, relevant laws, law enforcement profile, corruption profile, and prevalent culture and subcultures.

2.1.1 Technological Profile

2.1.1.1 Telecommunications

India has the second largest telecommunications market in the world [Krishna 2013] with over 864 million wireless cellphone lines and over 30 million landlines [TRAI 2013]. Youth make up the fastest growing segment of cellphone users in India [Krishna 2013]. Of subscribers in 2012, 44 million used smartphones [Meeker 2012], making India the third largest smartphone market in the world [Paczkowski 2013]. The majority of smartphones sold in India have the Android operating system [Singh 2012]. A September-October 2012 study by Nielsen Informate Mobile Insights across 46 cities and 10,000 users showed the operating systems as follows [Saxena 2013]:

- 62% Android
- 21% Symbian
- 13% Microsoft Windows or Microsoft Mobile

- 3% Research in Motion (RIM)
- 1% Apple IOS

RIM has released a smartphone, the BlackBerry Q5, aimed at developing countries [Krishna 2013, Connors 2013]. However, BlackBerry shipments to India have declined from 12.8% in 2010 to 5.9% in 2012 [Paczkowski 2013], while Apple's iPhone sales in India have increased more than 400% [SN 2013b]. Smartphone adoption in India may lead to a more productive workforce but can become another avenue for insider attacks. Organizations operating in India will need to be vigilant about protecting sensitive information on mobile devices.

India has a mixture of Global Systems for Mobile communications (GSM) and Code Division Multiple Access (CDMA) types of cellphone communications protocols [Bafna 2012]: GSM is the dominant technology with 72% of the mobile subscriber market [India Biz News 2012]. Out of India's 640 districts, 610 are covered by 3G services as of November 2012 [Bafna 2012, Shinde 2009]. The areas with 4G are few but include Kolkata and Bangalore [Sharma 2012a], and a handful of other cities are currently undergoing 4G rollouts [Bafna 2013, Times of India 2012]. Some cellphones in India are multiple Subscriber Identity Module (SIM) card hybrids, which allow both GSM and CDMA networks to be accessed, so the cheaper services can be used when available [Garyali 2013, Rana 2010, Mobile Indian 2013, Thomas 2011, LawTeacher 2013].

2.1.1.2 Internet

India continues to add internet subscribers [TRAI 2013]: Its internet penetration rate is approximately 11% [Meeker 2012]. Mobile internet usage is 59% versus 41% desktop internet usage as of December 2012. Mobile internet usage in India is higher than the global mobile usage of 14% [Meeker 2012]. India has 25.33 million internet users with connection speeds less than 256Kbps (2.1% of India's population) [TRAI 2013]. Broadband subscribers—those having greater than or equal to 256Kbps connection speeds—have been increasing and currently stand at 14.98 million subscribers (1.2% of India's population) [TRAI 2013]. Approximately 2.4% of the internet connections in India run faster than 4Mbps, and about 0.3% run faster than 10Mbps, with an average speed of 1.3Mbps as of the first quarter of 2013 [SN 2013b, Akamai 2013]. The number of connections above 10Mbps increased 102% of the last Quarter on Quarter [Akamai 2013]. This could potentially show increased interest in higher speed connections, as well as infrastructure improvements and costs that are acceptable to end users. Digital subscriber line (DSL) technology comprises 84.82% of broadband subscribers [TRAI 2013]. Furthermore, India has 16.2 million unique Internet Protocol Version 4 (IPV4) addresses in use [SN 2013b, Akamai 2013]. India may have a more robust internet infrastructure than other countries that rely on the South East Asia-Middle East-Western Europe 4 (SEA-ME-WE 4) connection undersea cable. On March 27, 2013, that cable was cut, causing outages or slow connections to Egypt, India, and Pakistan—all serviced by the connection. According to Akamai, India was affected the least [Akamai 2013], which may indicate the country has additional internet backbone connections that are more capable of handling infrastructure breakdowns. Currently, India has a lengthy repair time for undersea cables (sometimes over two months) due to bureaucratic hurdles [Thomas 2013] that include a relatively large number of clearances and required permissions. The Indian Telecommunications Ministry has proposed shortening undersea cable repair times to a more standard average of three to five days [Stern 2013]. The repair time can have a large effect on online connectivity from India to the

rest of the world; for instance, in December 2008, undersea cable breaks resulted in a loss of 50-60% of bandwidth connectivity for India [Rapp 2012].

2.1.1.3 Internet Security Threats

According to a 2013 study by the Symantec security company, India is home to 16% of computer viruses and globally ranks second in virus prevalence, just behind the United States. Malicious code is also an issue for India: India has the third highest rate of malicious code worldwide [Symantec 2013].

Distributed denial of service (DDoS) attacks cause organizations and individuals to experience slow or complete service outages. India experienced an uptick in source-IP attacker traffic in 2013. India ranked sixth at 2.6% of originating IP attack traffic in the first quarter of 2013, up from 2.3% in the fourth quarter of 2012 [Akamai 2013]. Attackers using IP addresses originating in India also targeted Transmission Control Protocol (TCP) port 1433, which is typically used for Microsoft SQL Server communications. This was the second most targeted port [Akamai 2013]. Increases in attacker traffic should concern India's citizens and government, and could indicate other issues within the country. For example, it may show that Indian citizens are, in fact, becoming the target of malware designed to conduct DDoS attacks on behalf of an attacker.

The National Technical Research Organisation [sic] (NTRO), which is similar to the U.S. National Security Agency (NSA) [Unnithan 2007], has attempted but failed to crack both a Google and a Skype server. However, it was able to gain access to Rediffmail (an Indian news and email website) and Sify (an Indian news website) for unknown reasons [Prakash 2013].

2.1.1.4 Privacy and Security

Recent revelations of the NSA's data collection program have brought to light other governments' activities. India's own collection activities are more far-reaching and comprehensive than the NSA's [York 2013]. Regarding the collection, India's Union Minister for External Affairs Salman Khurshid stated, "It is not snooping. It is only computer study and computer analysis of patterns of calls" [Prakash 2013]. Indian licensing law requires telecommunications companies to provide their data to the government without court processes [Prakash 2013, York 2013]. India does have a central monitoring system (CMS) in place that stores phone records in real time. The system allegedly can monitor, in real time, all mobile and fixed lines, and all internet users [Roy 2013]. India service providers cannot use bulk encryption. Furthermore, no person or entity can use an encryption key greater than 40 bits. Longer encryption keys require permission from the Indian Department of Telecommunications, and decryption keys must be supplied to that department [York 2013, Government of India 2013]. The use of small encryption keys could pose a serious threat to citizens and organizations in India, as well as to organizations that outsource to India and those with India in their supply chain. A malicious insider using well-known methods could decrypt communications secured with a 40-bit encryption key. Using 1997 technology, 40-bit Data Encryption Standard (DES) encryption was cracked within four hours by a graduate student at the University of California at Berkeley using a network of 250 computers [CNET 1997]. Given today's technology, it would be possible to crack a short key length using a single system in less time. Furthermore, an insider within the Department of Telecommunications who obtained access to the encryption key store could easily decrypt "secure" communications between individuals and institutions.

2.1.1.5 Social Media

Social media is used in India by individuals, businesses, and even some government organizations. Some Indian organizations and regions use social media to solicit feedback on changes in their locality and communicate with citizens. For example, the Municipal Corporation of Delhi receives feedback from citizens through its website, and the Delhi and Bangalore Police departments regularly use Twitter and Facebook. However, citizens apparently are not confident that their feedback is used [Sharma 2012b].

2.1.2 Relevant Laws

While some laws and regulations relevant to insider threat exist, they are often considered piecemeal rather than comprehensive [Shaw 2011]. Indian cybercrime studies indicate that malicious insiders are responsible for "69 percent of information theft" and "over one-third of the frauds" [Muthukumaran 2008]. Indian organizations face more incidents than just those caused by malicious insiders [Singh 2013]: Phishing attacks and lost or stolen devices are a growing problem, although they are beyond the scope of report [Muthukumaran 2008].

One of the primary laws used to address cybercrime is the Information Technology Act of 2000 (IT Act) [Indian Parliament 2008]. Potentially relevant provisions include prohibiting unauthorized access to and tampering of protected source code. Such prohibitions can be compared to the U.S. Computer Fraud and Abuse Act's prohibitions to unauthorized access to and damage of protected systems [USC 2013]. Similar to some U.S. data breach law, the IT Act allows a negligent organization to be found liable for failing to take reasonable security practices to protect data [IIBF 2005]. Unlike the United States, Canada, and many European nations, India is not a signatory of the Budapest Convention on Cybercrime [COE 2004]. (That convention is an international treaty seeking to address internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations [Council of Europe 2001].)

Privacy laws may also be of concern to organizations developing insider threat programs. Article 21 of the Constitution of India has been interpreted to provide the right of privacy to its citizens, a concept also present in other regulations [Shaw 2013, Shroff 2012, Ahman 2009]. In addition, the Indian government passed the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules legislation (heretofore called IT Rules), which regulate the collection, processing, and use of personal information by organizations [MCIT 2011]. Adopting a definition similar to that used in the EU's Directive 95/46/EC, the IT Rules define personal information as "any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person." These rules provide additional regulations for sensitive personal information, such as passwords, and financial and medical information [MCIT 2011]. An organization may hold many other assets besides personal information—for example, patents, trade secrets, geo-location or biometric data—and a variety of legal frameworks may be present to regulate what can be collected and how it can be used or stored. While the scope of this report does not allow for a detailed discussion of all these regulations, a few recent examples of how the Indian government collected biometric and telecommunications information illustrate some of the initiatives and regulations in this area [Bowe 2012, York 2013].

As shown in recent cases, employee-monitoring programs can implicate whistle-blowing activities [Lerner 2012]. While the Indian Constitution provides for freedom of speech, the state can restrict that freedom for reasons such as "public order," "decency or morality," and "friendly relations with foreign states" [Mehta 2013]. While a bill to protect whistle-blowers has been approved by India's Union Cabinet, legal observers have reservations about the level of protection [Collins 2010]. Unlike multinational corporations, many Indian companies do not have whistle-blowing policies because they are not required. In addition, whistle-blowers have historically faced harassment [Srivastava 2013].

Indian employment law is another area relevant to insider threats. One aspect of employment law is the regulation of background checks. While the United States requires some notification to consumers during the process of credit checks through its Fair Credit Reporting Act, India has no such regulation [Shroff 2012]. In addition, the U.S. Americans with Disabilities Act and the Rehabilitations Act contain certain regulations for performing and taking action on employee medical testing [DOJ 2009]. Although India has a Persons with Disabilities Act, its laws in this area are considered "less developed" than the United States' are, and some employers have conditioned employment on successful medical testing [Shroff 2012, Rao 2008]. In addition, Indian Constitution Article 15 prohibits state discrimination based on "religion, race, caste, sex or place of birth" [Government of India 1950]. However, Act 15 also states, "Residence as a qualification for certain purposes such as employment may not be classed with discrimination based on caste and place of birth" [Kumar 2011]. Women in the private workforce have some protections [Shenoy 2013] including the Persons with Disabilities Act [Medindia 1995], Industrial Law [Bhasin 2007], and the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act [Gopalakrishnan 2013]. Specific organizations in India require background checks, such as the Reserve Bank of India and Indian companies with an ISO 27001 certification. However, the lack of centralized and updated information can make conducting background checks difficult [Shroff 2012]. To alleviate some concerns about background checks for IT professionals, the Indian National Association of Software and Service Companies (NASSCOM) created a National Skills Registry, and other industries have followed suit [Shroff 2012, NASSCOM 2013]. Other potentially relevant employment regulations include the requirement for government permission prior to certain types of layoffs and the freedom of "association and collective bargaining rights" [IPTU 2011]. Due primarily to these regulations, Indian employment legislation for "regular" or "indefinite" contracts is considered some of the strictest in the developing world (and stricter than some of the developed world) [Dougherty 2008].

2.1.3 Law Enforcement Profile

India uses a complex law enforcement structure[6] that employs many people, like you might expect of a country with a large population and physical size [CIA 2013c]. However, there are few cybercrime investigative units within India's law enforcement structure [ISEA 2013]. For example, on December 18, 2000, the Cyber Crime Investigation Cell, Crime Branch, Crime Investigation Department was established to address cybercrime in Mumbai, India [CCIC 2013]. This is still the only such unit in Mumbai—India's most populated city [City Mayors Foundation 2012]. And one investigative unit in Bangalore (India's fifth most populated city [City Mayors Foundation 2012])

[6] http://en.wikipedia.org/wiki/Law_enforcement_in_India

provides the only cybercrime service to the entire Indian state of Karnataka [Naavi.org 2013], which comprises approximately 192,000 square kilometers of land [Mudde 2007]. Although India comprises 28 states and has a population of approximately 1.2 billion [CIA 2013c], it has only 21 cybercrime units [ISEA 2013].

According to the India National Crimes Records Bureau (NCRB), the number of cybercrime cases in 2012 rose by 46% in New Dehli, and 67% in Faridabad and Ghaziabad [NCRB 2012]. Therefore, it is not surprising that on July 31, 2013, the chief minister of the Indian state of Kerala announced the state government will set up 19 cybercrime investigative units to tackle the growing cybercrime-related incidents in the state—almost doubling the country's number of cybercrime investigative units. Each unit was authorized to have seven personnel. While this appears to be a step in the right direction, it still only constitutes 133 cybercrime personnel to cover an area of approximately 39,000 square kilometers and a population of 40 million people [Kerala.com 2013]. And some portion of those positions may turn out to be supervisory, management, and administrative, rather than all cybercrime investigators. Moreover, if all 21 of the pre-existing cybercrime investigative units also have only 7 personnel allocated, that equals a total of only 147 people investigating cybercrime—a low number for a country of 1.2 billion people.

India passed an Information Technology (IT) Act in 2000 to specifically address cybercrimes. It was amended in 2008 to add some offenses and civil liberty considerations, such as allowing bail for many more of the offenses. Also, the Act (as amended) does not cover the majority of crimes committed through mobile phones. According to the NCRB, 157 cases were registered under the Act in 2011, yet only 65 people were arrested [Zargar 2013].

According to the opinion of one cyber law and cybersecurity expert, "I would say it [the IT Act] is effective in metropolitan cities like Mumbai, Delhi, Hyderabad, Bhopal, Bangalore, etc., but it is feeble in tier-two level cities as awareness of the law by enforcement agencies remains a big challenge" [Zargar 2013].

In the area of cyber forensics, we found few examples of widespread use or professional competence in Indian law enforcement: One of them was the Resource Centre for Cyber Forensics – India, created in August 2008 to develop cyber forensic hardware and software tools [Resource Centre for Cyber Forensics 2013]. However, we found that most of the other available cyber forensics expertise was outside of law enforcement and instead in private practices, such as consulting and cyber forensics businesses in India.

According to a cybersecurity expert interviewed anonymously for this report, most companies do not involve the police in cybersecurity cases. The police have been known to confiscate entire computer systems (including the monitors and keyboards) rather than just making a forensic image of the system memory and hard drive. Also, cybersecurity-related cases take companies a long time and a lot of money to pursue.

For now, companies are likely to rely on private consultants and incident response businesses to help them identify and remediate cybercrimes perpetrated by trusted insiders. Companies in India need to carefully consider and develop robust non-law-enforcement options for preventing, detecting, and responding to such crimes.

2.1.4 Corruption Profile

India comprises 28 states and 7 union territories and has a population of 1.2 billion. But because it contains only five major urban areas [CIA 2013c], discovering variations in levels of corruption and anti-corruption across the country might be possible. However, for the purpose of this overview, we consider India a single holistic country unless specifically noted.

India has a poor score on the Corruption Perceptions Index (CPI) for 2012, which measures the perceived levels of public sector corruption in 176 countries and territories around the world on a scale of 0 – 100, with 100 representing no corruption. India, with a score of only 36, tied with 7 other countries as the 94th ranked country in the index. This means that India's perceived public sector corruption is in the bottom 47% of the index, or worse than 53% of all the countries measured [Transparency International 2012].

Perception is important in enhancing business opportunity and investment in a country's market. However, even though corruption in India is rated as moderately high, the United Nations Conference on Trade and Development revealed that India is still the second most popular country for foreign direct investment [UNCTAD 2012]. This may indicate that investors have accepted corruption as a mainstay of the Indian culture and that businesses knowing how to participate effectively in corruption can still thrive. This view may be supported by statements of thought leaders on corruption in India, such as Mr. Ratan Tata, chairman of the Tata Group, who opined that businesses that choose not to participate in corruption will "...leave behind a fair amount of business" [Hindu Business Line 2011].

Recent anti-corruption efforts in India reveal that anti-corruption laws are largely ineffective and lack the significant punishments used by other countries [Goel 2012]. A survey by Transparency International revealed that 44% of Indians viewed the government's actions to fight corruption as "ineffective," while only 25% thought they were "effective" [Transparency International 2013a]. The 2010 Global Corruption Barometer revealed that corruption is a daily struggle for Indian citizens, wherein 54% of households say they have had to pay bribes to receive basic government services [Transparency International 2013b].

A KPMG survey of corporate executives in India revealed that 68% believed that many cases of public corruption were induced by the private sector [KPMG 2011]. And according to the KMPG 2010 India Fraud Survey, 42% of respondents believed that bribery had become acceptable behavior, and 38% said that bribery was an integral way of getting things done in their industry [KPMG 2010].

Anti-corruption in India is also hampered by its segmentation by states. Each has its own Lokayukta (ombudspersons) [Jain 2003], and many critics believe those individuals lack sufficient authority to provide any real anti-corruption enforcement. Additionally the Lokayukta in each state are set up based on its particular law, resulting in no uniform jurisdiction across the country. The Lokayukta are also widely seen as only "ceremonial" positions and "post-retirement employment for Judges" [Sharma 2011]. Ironically, one Lokayukta from the Indian state of Kanataka (where the city of Bangalore is located) had to resign after only 47 days in office because of allegations of corruption [Gowda 2011].

Numerous stories of corruption in India, coupled with a lack of an effective anti-corruption capacity, pose at least two major implications for cybersecurity policy and practice:

- Adroitly applied corruption could shield actual cybersecurity flaws from discovery by supposedly independent auditors.
- Potentially, corruption could be used to hide draconian, so-called cybersecurity implementations that actually violate privacy, civil liberties, or other laws and protections.

2.1.5 Prevalent Culture and Subcultures

The Republic of India is a democratic nation, the seventh largest country in the world by area, and the second largest by population: 1,220,800,359. India's labor force is the second largest in the world at 498,400,000 [CIA 2013a]. The country comprises four geographic regions: Northern India which includes the Capital (around Delhi), Western India, Southern India, and Eastern India.

It is a country steeped in a rich and diverse cultural landscape of histories, beliefs, and traditions that have contributed to cultural heterogeneity and a multilingual society. This is exemplified by strong regional cultures and identities that are often linked to geography, and to linguistic and religious affiliations [LaDosa 2006, Mitchell 2009].

The Constitution of India recognizes 18 languages as scheduled languages and 48 as non-scheduled or minority languages [Pandharipande 2002]. According to Ethnologue, India has 454 living languages currently in use as a first language. India's linguistic diversity is ranked high: It is positioned as number 14 on Greenberg's language diversity index and has an assigned value of 0.916, with 1 being the highest diversity and 0 being no diversity [Ethnologue 2013].

While India has a heterogeneous cultural and linguistic landscape, it does share some broad, homogeneous, culturally significant characteristics. Note, however, that the cultural considerations and implications put forth here are broad generalizations for the purposes of this report. Because no society or culture is homogeneous, exclusions from or variations to the generalizations we posit here are to be expected.

How people communicate can provide great insights into their culture. According to Hall, when communicating, "Meaning and context are inextricably bound up with each other," and thus it is important to examine meaning and context together [Hall 1976]. To give voice and insight into the sociocultural aspects of communication, Hall created the high-low context continuum that places cultures along a dimension spanning from high-context to low-context [Hall 1976]. Also culturally relevant is how people perceive and organize time and space. Those perceptions are a sociocultural construct that influences our daily lives, how we interact with others, and how we perceive our past and future. Based on ethnographic research, Hall proposed two variant solutions of how time and space are culturally organized: monochronic time and polychronic time [Hall 1976]. The high-low context continuum, and monochronic and polychronic views of time and space provide a framework for understanding culturally significant differences between cultures.

Another measure that can provide broad generalized insights into the sociocultural construct of a country is Hofstede's dimension of individualism and collectivism [Hofstede 2010]. Individualism and collectivism each represent a set of distinguishing values, and the positioning on the dimension reflects a focus of either "I" (the individual) or "we" (the collective group). On a scale of 0 to 100, the most collectivistic countries are closest to 0, and those with high individualistic traits

are closer to 100. India is positioned at 48 on Hofstede's scale of national culture, which places it firmly as collectivistic [Hofstede 2010].

In broad general terms, India is high-context and collectivistic, and has a polychronic perception of time and space. In high-context cultures, cultural knowledge is implicit, and contextually bound non-verbal aspects of communication are important, such as the gestures, body language, facial expressions, tone of voice, body proximity, and silence that all accompany the explicit verbal code, that is, the words themselves [Hall 1976].

Interpersonal relationships and trust are important to all aspects of life in high-context and collectivistic societies. Behavior in collectivistic cultures is governed by in-group norms with a focus toward the good of the collective group versus the good of the individual. Collectivistic cultures value a sense of self-respect and having the acceptance and approval of one's peers, supervisors, and family members. Conflict can arise from the violation of boundaries, norms of group loyalty and commitment, reciprocal obligations, and trust. When dealing with conflicts or problems, high-context, collectivistic societies focus on the social aspects and implications of a problem [Guess 2004]. According to Guess, they value security (of the group), are more risk-avoiding, and follow passive, collaborative, and avoidance strategies.

Cultures such as India with polychronic tendencies see time as fluid and flexible. Time is adjusted to fit the needs of the person and not viewed as a thing that can be compartmentalized or wasted [Hall 1976]. Other polychronic markers include handling multiple tasks simultaneously, accepting late arrival to meetings or events, and high tolerance for interruptions [Hall 1976]. The overall focus is on relationships and people, which reinforces the high-context and collectivistic nature of Indian society.

A societal concern relevant to the study at hand is corruption and fraud, which appear to be embedded in political, economic, and sociocultural facets of Indian society [KPMG 2012, Mathur 2012, Mazzarella 2010]. Bribery and fraud in their various forms may, in part, be a reflection of the collectivistic nature of Indian society and its reliance on the collective group, relationships, and reciprocal obligations. The level of corruption and bribery in a country as well as the extent of its identification and prosecution may indicate the level of sociocultural tolerance for such practices and how engrained such practices are in its sociocultural fabric.

As mentioned earlier in this report, India's CPI score in 2010 was 36, indicating a moderately high level of perceived corruption [Transparency International 2012]. A common form of corruption in India is bribery, which takes place anywhere from small rural villages to large corporations [KPMG 2012, Mathur 2012, Mazzarella 2010]. According to the KPMG India Fraud Survey 2012, the organizations polled were split down the middle as to whether business could be done without paying bribes: 50% said yes and 50% said no [KPMG 2012]. For additional information on corruption and bribery in India, see Section 2.1.4.

Indian culture on a national and regional level may serve as an influencing force for the culture found in organizations, that is, organizational culture. However, the organizational culture and practices within countries have been known to deviate from the norm [Hall 1976]. According to Hofstede and Minkov, "In practice there is a wide range of types of employer-employee relationships within collectivistic and individualistic societies" [Hofstede 2010]. When employers operate outside the collectivistic norm, it may potentially impact employees' loyalty and therefore their

actions. This is an example of conflict and the results of not conforming to societal norms of trust, loyalty, and reciprocal obligations [Guess 2004].

Because of the strength of the regional cultures in India, differences at the regional level are to be expected that encompass regional variations of customs, values, beliefs, behaviors, and so forth. Crosscutting differences might also be found by industry and profession. While exceptions to the generalizations are likely, the organizational culture of Indian institutions operates under the influence of high-context, collectivistic, and polychronic tendencies, and to some degree should reflect that influence.

2.2 Analysis of Implementation of Five Best Practices in India

In this section, we analyze implementation in India of five best practices against insider threat. We focus on implementation issues that arise due to the nation's relevant laws, technological profile, law enforcement profile, corruption profile, and prevalent culture and subcultures. We selected these best practices for analysis from the *Common Sense Guide to Mitigating Insider Threats*, out of its recommended 19:

- Practice 16: Develop a formalized insider threat program.
- Practice 13: Monitor and control remote access from all end points, including mobile devices.
- Practice 4: Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.
- Practice 18: Be especially vigilant regarding social media.
- Practice 9: Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.

2.2.1 Practice 16: Develop a formalized insider threat program.

For a summary of this best practice, see the appendix on page 64.

2.2.1.1 Effects of India's Technological Profile

Part of an insider threat program requires maintaining the confidentiality of all related information. This includes securing all communications with encryption. Encryption keys should be protected from unauthorized access or disclosure, and should be strong enough to withstand cryptographic attacks.

India's government requires cryptographic keys longer than 40 bits to be placed on file with the Department of Telecommunications [MCIT 2011]. Forty-bit encryption keys are weak and pose a danger to protecting the confidentiality and privacy of an inquiry or investigation. Someone determined to discover the proceedings of an investigation could crack the encryption in a short amount of time. Furthermore, a malicious insider within the Department of Telecommunications who has access to the strong encryption keys could use them to compromise an inquiry within the department's organization or could be bribed to provide the encryption keys to an outsider.

2.2.1.2 Effects of India's Laws

When implementing an insider threat program, an organization may consider what privacy and security protections it will put in place. India has legislated specific requirements for companies

processing personal information, with additional requirements for sensitive information [MCIT 2011]. Requirements include a published privacy policy, written consent for the collection of sensitive data, and reasonable security practices [MCIT 2011]. ISO 27001 is one standard that will satisfy the reasonable security requirements [MCIT 2011]. Some exemptions to the IT Rules exist for outsourcers, that is, organizations that do not obtain sensitive information directly [Hunton & Williams 2011b]. In addition, varying and sometimes inadequate security standards do exist, such as in the case of data encryption. As noted by the Data Security Council, when referencing government encryption standards under the IT Act, "Encryption policy under this section is urgently required as a national policy, since at present encryption is restricted to 40-bits under the telecom licensing policy regime. This level of encryption is weak, and does not promote client confidence… DSCI has engaged with the government to help formulate the encryption policy" [DSCI 2013]. One author notes, "Encryption in India is a hotly debated and very confusing subject. The government has issued one standard, but individuals and organizations follow completely different standards" [Hickok 2011]. Conflicting standards could affect implementation of certain insider threat prevention practices (e.g., data classification/management).

While the recent IT Rules may add some privacy and security requirements, one recent report notes that there "is no law in India governing the extent to which employers are allowed to monitor their employees….Courts have not so far dealt with this issue in a general way, perhaps because the legal framework to bring such an issue does not exist" [Privacy International 2012]. While monitoring may be restricted in some private areas, employers may generally conduct surveillance [Privacy International 2012]. A few court cases have prevented specific types of information such as pregnancy or HIV status from being collected in public employment or civil service [Privacy International 2012]. Finally, another aspect of an insider threat program is the ability to respond, sometimes through law enforcement, to the crimes. India does have specific cybercrime laws that may allow for the prosecution of malicious insider crime [Indian Parliament 2008]. Also, as discussed in Section 2.1.2, India does not yet have specific whistle-blower regulations in place [Collins 2010].

2.2.1.3 Effects of India's Law Enforcement Profile

From the U.S. perspective of this best practice, the CSG recommends making a formalized response plan part of an insider threat program [Silowash 2012]. That plan would likely include how and when to engage with law enforcement for cyber-related insider threat incidents. In India, companies may want to consider engaging with private consultants or businesses that specialize in cyber forensic incident response, at least for the initial part of the response plan, rather than directly involving local law enforcement.

An insider threat program should take into account the fact that there are few cybercrime investigation units in India's law enforcement structure [ISEA 2013]. For more information about those units, see Section 2.1.3.

Because most companies do not involve the police in cybersecurity cases and, when they do, whole computer systems are often confiscated (see Section 2.1.3), an organization could potentially lose access to important data needed to function and make money. This is one reason that an insider threat program might plan to avoid involving law enforcement, where legal to do so.

Companies in India should carefully consider and develop robust non-law-enforcement options for preventing, detecting, and responding to threats from malicious insiders.

2.2.1.4 Effects of India's Corruption Profile

Public sector corruption in India is considered quite high when compared to other countries [Transparency International 2012]. Insider threat programs within government agencies should be vigilant in detecting and responding to bribery, which is widely considered to be an integral way of getting things done in India [KPMG 2010]. The 2010 Global Corruption Barometer revealed that corruption is a daily struggle for Indian citizens, wherein 54% of households say they have had to pay bribes to receive basic government services [Transparency International 2013b]. Therefore, an effective insider threat program, both in the government and in the private sector, should include mechanisms of checks and balances to ensure that bribery and other corruption have not influenced its ability to prevent, detect, or respond to legitimate insider threats [Transparency International 2013b].

2.2.1.5 Effects of India's Prevalent Culture and Subcultures

Because India has a heterogeneous cultural landscape with strong regional cultural affiliations, organizations should consider the various cultural contexts in which they operate including but not limited to national, regional, industrial, and professional when developing a formalized insider threat program [LaDosa 2006, Mitchell 2009]. Also relevant would be the culture of the organization, its values, beliefs, and so forth. To increase the success of a formalized insider threat program, the organization should consider the organizational culture when developing the program to increase the chance of its adoption and institutionalization.

Cultural differences, position on the high-low context continuum, and degrees of collectivism and individualism may also deviate from the norm within organizations at the individual and group level. These differences may occur as a subculture associated with profession, gender, language, or religion. It is important to consider the potential cultural diversity within an organization and the external complex influences when developing a formalized insider threat program. Generally speaking, India is a high-context culture in which 454 languages are used. Communication in high-context cultures is indirect and highly dependent on cultural context. To ensure effective communication of an insider threat program and its associated policies, processes, and procedures, an organization should consider the linguistic diversity, modes of communication, and high-to-low-context aspects of communication that might be present in those covered by the program.

Although India is a collectivistic culture, there may be individuals within any country or organization whose positioning on the collectivistic and individualistic scale may vary. In collectivistic cultures, behaviors tend to be governed by in-group norms with a focus on the collective group [Guess 2004]. When developing guidelines and scenarios for a formal insider threat program, organizations should consider the collectivistic nature of India to increase the chances of having suspicious behavior reported. Individuals who have strong collectivistic tendencies may be hesitant to report suspicious behaviors of co-workers. Because trust and loyalty—including that between employees, and between the employer and its employees—are important characteristics of collectivistic cultures organizations should consider these factors when developing, deploying, and communicating their insider threat programs [Guess 2004].

2.2.2 Practice 13: Monitor and control remote access from all end points, including mobile devices.

For a summary of this best practice, see the appendix on page 64.

2.2.2.1 Effects of India's Technological Profile

The CSG says that remote access from any device needs to be carefully monitored and controlled [Silowash 2012]. Organizations need to understand all entry points into their systems and implement mitigating controls to protect systems from malicious insiders. The network perimeter is blurred when mobile devices are permitted to connect to an organization's information systems. These lines become particularly blurred when personally owned devices are introduced into the mix.

India's internet penetration rate is only about 11%. As such, an individual working in the cybersecurity industry within India (anonymized, whom we interviewed for this report) noted that more people have cellphones than computers and that cyber cafés were used too. According to Symantec, "India continues to rank high in the list for even the most basic threats, pointing to an urgent need for improved awareness levels and security measures, even as the country's adoption of internet and mobile technologies is on the rise" [Symantec 2013]. Therefore remote access to an organization's infrastructure may occur from a less secure location, such as a cyber café. Using a malware-infected computer could cause a security incident within the organization. Mobile devices are very popular in India, which has the second largest telecommunications market in the world. Mobile internet traffic accounts for 59% of all internet traffic there. According to Symantec's mobility survey, "72% of Indian businesses faced mobility incidents due to malware infections, spam incidents, exposures of information, breach of information due to lost/stolen devices and phishing/social engineering instances" [Symantec 2013].

Organizations operating in India or with India as a trade partner need to recognize the risks associated with mobile devices, including their capabilities and access to corporate networks from anywhere with a cellular or wireless signal. For example, India has 44 million smartphone users [Meeker 2012], and nearly all smartphones are equipped with cameras (video and/or still) or audio-recording capabilities. These features could enable a malicious insider to exfiltrate sensitive information, such as intellectual property. Studies have shown that malicious insiders account for 69% of information theft [Muthukumaran 2008].

Organizations should carefully control mobile devices used by their employees, contractors, and business partners, and by those visiting their facilities, especially if the devices will be processing sensitive information or be used in sensitive areas of the organization. Furthermore, organizations should consider implementing controls that prevent employees from accessing corporate networks using cyber café equipment to prevent possible malware infections or data leakage. Additional controls will be needed to ensure that all company information is destroyed on mobile devices and accounts are disabled when an individual leaves the organization. Organizations should also consider the encryption strength used for any virtual private network (VPN) connections. Due to India's government requiring encryption keys to be a maximum of 40 bits (without placing stronger keys on file) [York 2013], remote network connectivity may be susceptible to attack.

2.2.2.2 Effects of India's Laws

One recent movement that may affect this practice is "bring your own device" (BYOD), in which employees bring their own mobile devices, laptops, or other such devices, and use them at work. Such practices may have implications with respect to an employer's ability to monitor the devices. Recent media reports indicate that many Indian workplaces are considering the move to BYOD [Information Week 2013]. Few specific technical or privacy regulations appear to exist that would restrict this type of monitoring or control. Some of the data may be considered personal or even sensitive, in which case the employer would have to follow the IT Rules. As Stanton and Stam note, "Employee monitoring and surveillance in emergent industrial economies such as India and China also appear to be widespread but definitive figures from these countries are more difficult to obtain" [Stanton 2006].

2.2.2.3 Effects of India's Law Enforcement Profile

The CSG recommends the following for this best practice: "As much as possible, access to data or functions that could inflict major damage to the company should be limited to employees physically located inside the workplace. Remote system administrator access should be limited to the smallest group practicable, if not prohibited altogether" [Silowash 2012]. This advice is especially poignant for companies operating in India. Although the IT Act addresses many cybercrimes, it does not cover the majority of crimes committed through mobile phones [Zargar 2013]. Remote cyberattacks that are illegal in India (other than those orchestrated through mobile phones) are unlikely to be investigated or brought to trial due to India's low number of cybercrime investigation units [ISEA 2013]. Companies in India should carefully consider and develop robust policies to control remote access, since law enforcement in India is not likely to be a viable deterrent.

2.2.2.4 Effects of India's Corruption Profile

In 2011, the software piracy rate for India was 63% [BSA 2013b], indicating it is certainly a widespread problem there [Rangaswamy 2007]. Pirated software could introduce an unmanaged cybersecurity risk especially because it is often not eligible for software patches and bug fixes that can ameliorate known security vulnerabilities [CCIC 2013]. Organizations in India may be unable to effectively monitor and secure end points if pirated software is used by employees, due to the increasing proliferation of mobile platform malware.

2.2.2.5 Effects of India's Prevalent Culture and Subcultures

In collectivistic cultures such as India, monitoring and controlling remote access from all end points, including mobile devices, may be perceived or interpreted by some employees as the employer's lack of trust or loyalty. Trust and loyalty is important in collectivistic countries, including trust and loyalty between employee and employer. When employees think their employer has operated outside the collectivistic norm, it could potentially impact their loyalty and therefore their actions [Hofstede 2010]. Organizations should consider pointing out to their employees that monitoring and controlling remote access from all end points is beneficial to the group as well as the organization. Group-level incentives may influence compliance, acceptance, behaviors, and actions associated with monitoring and control.

2.2.3 Practice 4: Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.

For a summary of this best practice, see the appendix on page 63.

2.2.3.1 Effects of India's Technological Profile

Organizations operating in India should consider implementing additional monitoring capabilities in order to detect and prevent malicious insiders. Organizations may find it beneficial to implement additional monitoring (within legal authority) during probationary periods or with positions that have high turnover rates. Given India's weak encryption requirements, organizations may find it easier to monitor encrypted electronic communications because decrypting the communications would be relatively easy and decrypted communications could be more thoroughly analyzed as part of the monitoring process. However, technology that enables employee monitoring may be unaffordable for smaller organizations, given the average small business owner's financial means in this developing country. The CSG recommends that organizations review logs on a regular basis in order to detect and respond to possible malicious behavior [Silowash 2012].

2.2.3.2 Effects of India's Laws

Background checks are one key part of the hiring process, but they can be difficult in India due to the lack of centralized and updated information [Shroff 2012]. Efforts such as the National Skills Registry for IT professionals can possibly help [Shroff 2012]. However, reports indicate that resumé fraud is a serious problem in India: "One in 10 job applicants were estimated…to have committed background fraud" [Kumar 2013a]. Beyond simply lying on a resumé, full counterfeit businesses allow for candidates to pay for false experience certificates [Kumar 2013a].

Monitoring and responding to suspicious behavior can potentially implicate discrimination prohibitions because different cultures may behave in ways that can be viewed by other cultures as unusual. Ensuring that monitoring programs account for these differences in culture is important for appropriately detecting insider threat and addressing any discrimination prohibitions. Some discrimination protections exist, although they appear to focus predominantly on state employment [Government of India 1950, Shenoy 2013].

2.2.3.3 Effects of India's Law Enforcement Profile

The CSG recommends that, in the United States, employers use records of convictions rather than arrests when making hiring decisions [Silowash 2012]. As noted in the CSG, the U.S. Equal Employment Opportunity Commission (EEOC) states, "The fact of an arrest does not establish that criminal conduct has occurred" and "A conviction record will usually serve as sufficient evidence that a person engaged in particular conduct" [EEOC 2012]. That being said, the EEOC does not go so far as to suggest that arrest records cannot be used: It does state, "As a best practice, and consistent with applicable laws, the Commission recommends that employers not ask about convictions on job applications and that, if and when they make such inquiries, the inquiries be limited to convictions for which exclusion would be job related for the position in question and consistent with business necessity" [EEOC 2012]. This is an interpretation of U.S. equal employment law by the body that enforces the law—the EEOC. While we didn't find any evidence that such a policy is a best practice in India, the reasoning behind not using previous arrest records could apply: Conviction is an indicator of the individual having done a crime, whereas arrests may not be

sufficient evidence of criminal behavior. Related analysis done by the CERT Division has shown that, in the United States, the previous arrest (any arrest pre-IT sabotage attack) rate of insider IT saboteurs was the same as that of the average adult population of the United States [Silowash 2012, p. 25]: In other words, looking at previous arrest rates as part of a background check would not have helped to avoid insider IT sabotage in the United States, even if it had been legal. Further research would be needed to determine whether, in India, arrest records might have a correlation with the likelihood of an individual committing an insider cyberattack.

Indian law enforcement has not been widely effective when it comes to cybersecurity crimes. According to India's NCRB, in 2011, only 157 cases were registered under the IT Act (as amended), and, of those cases, only 65 people were arrested [Zargar 2013]. Therefore, the absence of conviction records in India should not be considered a reliable indicator during the hiring process. In addition, since there are only 21 law enforcement cybercrime investigation units [Zargar 2013] in the entire country, relying on law enforcement may not be a viable strategy for investigating suspicious cyber behavior. Companies may want to establish a relationship with a private consultant or forensic business that can help them resolve observed suspicious cyber activity.

2.2.3.4 Effects of India's Corruption Profile

Another aspect of corruption in India is the high level of occupational fraud by employees, through which Indian businesses lose about 4,000 crore (approximately $689M USD) each year [Varshney 2013]. This trend appears to be even more prevalent in the IT industry [Kumar 2013a]. Companies should consider exercising extra diligence when verifying employment histories and purported education and skills.

2.2.3.5 Effects of India's Prevalent Culture and Subcultures

Because trust and loyalty are important to collectivistic countries such as India [Hofstede 2010], the effect on the individual employee should be minimized by ensuring that background checks conducted during the hiring process are performed according to organizational policies and privacy rules and laws. Periodic reinvestigations, monitoring, and responding to suspicious or disruptive behavior might be viewed as an employer's lack of trust or loyalty. Organizations could mitigate that by ensuring employees understand the benefits these practices provide to both the group and the organization. After identifying suspicious or disruptive behavior, an organization may benefit by showing how the action impacted the larger group, without naming the individual involved.

2.2.4 Practice 18: Be especially vigilant regarding social media.

For a summary of this best practice, see the appendix on page 64.

2.2.4.1 Effects of India's Technological Profile

Given India's internet penetration rate of 11% [Meeker 2012], the highest internet usage may occur in highly populated areas or business centers. One individual working in the cybersecurity field in India, whom we interviewed anonymously for this report, stated that he believes most adults use their computer at work for personal purposes, as well as work. Therefore, organizations should offer security awareness training that includes social media guidelines. In particular, social media training should include social engineering awareness and the dangers of publishing too

much information online. Furthermore, some social media sites may open the organization to malware attacks. As noted in Symantec's Internet Security Threat Report, India's users lack protection from the most basic threats [Symantec 2013]. Up-to-date antivirus software should be deployed at both the network and end-point level to mitigate malware risks.

2.2.4.2 Effects of India's Laws

In India, social media is considered to be gaining "a firm foothold" in the workplace, with most of those surveyed approving the use of personal social media at work [Hindu Business Line 2012]. One report notes that there are "no specific legal restrictions against monitoring social network use." However, notifying employees of monitoring practices is a recommended and common practice [Proskauer 2012].

2.2.4.3 Effects of India's Law Enforcement Profile

The CSG recommendations for this best practice reflect a U.S. position that may not be as restrictive when designing social media policies and practices that employers follow in India [Silowash 2012]. A large concern with social media (from the perspective of this best practice) is the possibility of social engineering attacks on employees and the organization. An organization should take into account the recent rise of cybercrime in India. According to India's NCRB [NCRB 2012], in 2012, cybercrime cases increased by 46% in New Dehli and by 67% in Faridabad and Ghaziabad. These statistics are fairly representative of all the metropolitan areas in India, so an organization should consider expending extra effort to train employees to avoid common social media mistakes that empower social engineering attacks. Although there are comparatively few cybercrime investigative units in India (21 for the whole country) [ISEA 2013], more are being planned in some Indian states. However, organizations should consider contacting their supporting cybercrime investigative unit and establishing frequent liaison to stay current on new cybercrime trends in social media and get help when law enforcement response is needed.

2.2.4.4 Effects of India's Corruption Profile

Although government anti-corruption efforts in India are largely ineffective, there has recently been a large grassroots anti-corruption movement [Goel 2012]. While that movement has sometimes worked through formal channels, it has also leveraged social media to expose allegations of corruption. Organizations should consider how social media could help them either prevent or detect organizational corruption that could affect their cybersecurity posture.

2.2.4.5 Effects of India's Prevalent Culture and Subcultures

To address the collectivistic tendencies of Indian culture, an organization may consider including examples of how violating social media policies and practices could impact the good of the group as well as the individual. To increase compliance and institutionalization of social media policies and procedures, the organization should consider the organizational culture—and the various cultures represented in the workforce—when developing policies, procedures, and training materials. In high-context cultures when communicating, the contextually bound non-verbal aspects such as gestures, body language, facial expressions, and tone of voice that accompany words are themselves of importance [Hall 1976]. Additionally, because India has great linguistic diversity, organizations can ensure effective communication of social media policies, procedures, and cybersecurity risks by ensuring the language and modes of communication consider that diversity and the

high-to-low-context aspects of communication that might be present in those covered by the program.

2.2.5 Practice 9: Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.

For a summary of this best practice, see the appendix on page 63.

2.2.5.1 Effects of India's Technological Profile

Encryption of data in motion (DIM) and data at rest (DIR) while using cloud resources is one part of protecting the confidentiality and integrity of data in the cloud. However, India's requirement that all encryption keys larger than 40 bits be placed on file with the government [York 2013, Government of India 2013] can create risks for organizations attempting to secure their data in a cloud, particularly if it is hosted in India.

Data hosted in the cloud is under the care of a third party. Malicious insiders who work for the cloud services provider (CSP) might be able to access the data stored in the cloud due to the weak cryptography that may be implemented. Furthermore, if the company used stronger keys and stored them with the Department of Telecommunications, malicious insiders working in the Department might be able to obtain the encryption keys. To be successful, this scenario requires collusion of a malicious insider at either the organization or hosting provider, but the current corruption within the government makes it possible.

2.2.5.2 Effects of India's Laws

Symantec recently noted, "The use of cloud computing in India is still not clearly defined or accepted" [Routley 2013]. Problems appear to arise from the lag between the development of new technology and its associated regulation, and issues with developing the cloud computing model [Routley 2013]. The applicability of current Indian privacy and information security laws is potentially unclear with respect to the cloud [Ryan 2011]. However, companies have discussed potentially relevant legislation including the IT Rules and industry-specific laws in the banking and credit fields [Routley 2013].

2.2.5.3 Effects of India's Law Enforcement Profile

Companies should be careful to consider which law enforcement jurisdictions will apply to their cloud services business partners. Although the IT Act strengthened Indian law enforcement's ability to handle cybercrimes, the law is not necessarily understood or applied equally throughout the country. According to the opinion of one cyber law and cyber security expert, "I would say it [the IT Act] is effective in metropolitan cities like Mumbai, Delhi, Hyderabad, Bhopal, Bangalore, etc., but it is feeble in tier-two level cities as awareness of the law by enforcement agencies remains a big challenge" [Zargar 2013].

Organizations should ensure that their cloud service contracts clearly articulate all their expected cybersecurity standards and should not rely on provisions of the IT Act being sufficiently understood or applied. India's law enforcement is unlikely to uphold those service level agreement (SLA) contracts (even if standards are fully articulated), because there are so few cybersecurity-savvy law enforcement personnel to cover the large Indian population. As a result, organizations should consider alternative methods of enforcing those agreements. For instance, respected inter-

national standards bodies that can do unannounced checks could be an effective control for India because of the possible financial losses (due to fines or due to loss of business resulting from certification loss) to the company if the check fails: A financial incentive or risk might be a stronger motivator than concern about unlikely law enforcement.

2.2.5.4 Effects of India's Corruption Profile

The CSG recommends that organizations strictly enforce supply chain management, assess suppliers, and ensure transparency in overall information security and management practices [Silowash 2012]. However, the high level of corruption in India, specifically manifested through bribery, has been inculcated in the Indian business world. Based on the results of the KPMG 2010 India Fraud Survey [KPMG 2010] we discussed in Section 2.1.4, organizations should consider how corruption could impact their cloud services. As one possible mitigation for corruption, organizations may want to include provisions in their cloud services contracts for requesting security audits of their trusted business partners. These audits could be both scheduled and spontaneous in order to strengthen confidence in their results.

2.2.5.5 Effects of India's Prevalent Culture and Subcultures

Cloud services may be provided by organizations that reside in countries with cultures different than India's. To avoid any culturally based misunderstanding, an organization should consider the high-low context continuum, and various individualistic and collectivistic characteristics when developing its policies, practices, and training materials [Hofstede 2010, Hall 1976]. For instance, a U.S.-based CSP might take an SLA literally since the United States has a generally low-context culture. However, that CSP might need to adjust its policies, practices, and training materials so its SLAs in India (generally a high-context culture) proceed as the CSP expects.

2.3 Summary of Best Practice Implementation in India

In the tables that follow, we summarize our findings for India for all issues identified for all factors except laws and provide recommendations for effective cybersecurity practice implementations despite those issues.

.

Note: Because the CERT Division does not give legal advice, this table does not include legal issues and recommendations.

Cybersecurity Best Practice	Problems or Potential Problems for Implementing Best Practices	Recommendations
India - Technology		
CSG best practice 16	India's government requires cryptographic keys longer than 40 bits to be placed on file with the Department of Telecommunications. As a result, many organizations might choose to use keys that are 40 bits or shorter, which are weak and pose a danger to protecting the confidentiality and privacy of an inquiry or investigation.	Consider risks from weak keys anyone could attack versus risks from government insiders (or persons colluding with government insiders). Protect encryption keys from unauthorized access or disclosure, and consider making them strong enough to withstand cryptographic attacks (which requires using long keys). Although risks from government insiders would remain, these actions counter other risks (and if the key was weak, both government and non-government insiders might be able to get access to the data).
	A malicious insider within the Department of Telecommunications who has access to the strong encryption keys could use them to compromise an inquiry within the department's organization or could be bribed to provide the encryption keys to an outsider.	Consider risks from weak keys anyone could attack versus risks from government insiders (or persons colluding with government insiders).

Cybersecurity Best Practice	Problems or Potential Problems for Implementing Best Practices	Recommendations
CSG best practice 13	India's internet penetration rate is only about 11%, so remote access to an organization's infrastructure may occur from a less secure location, such as a cyber café or cellphone. Organizations operating in India or with India as a trade partner need to recognize the risks associated with mobile devices, including their capabilities and access to corporate networks from anywhere with a cellular or wireless signal. The network perimeter is blurred when mobile devices are permitted to connect to an organization's information systems—especially when employees use personally owned devices.	Carefully monitor and control remote access from any device. Understand all entry points into your systems and implement mitigating controls to protect those systems from malicious insiders.
	India has 44 million smartphone users, and nearly all of those devices are equipped with cameras or audio-recording capabilities. These features could enable a malicious insider to exfiltrate sensitive information; malicious insiders account for 69% of information theft.	Carefully control mobile devices used by your employees and by those visiting your facilities, especially if the devices will be processing sensitive information or be used in sensitive areas of the organization. Consider implementing controls that prevent employees from accessing corporate networks using cyber café equipment to prevent possible malware infections or data leakage. Use additional controls to ensure that all company information is destroyed on mobile devices and accounts are disabled when an individual leaves the organization.
	India's government requires encryption keys to be a maximum of 40 bits, making remote network connectivity susceptible to attack.	Consider the encryption strength used for any virtual private network (VPN) connections.
CSG best practice 4	Given India's weak encryption requirements, organizations may find it easier to monitor encrypted electronic communications.	Consider implementing additional monitoring capabilities in order to detect and prevent malicious insiders early on. Implement additional monitoring (within legal authority) during probationary periods or with positions that have high turnover rates.
	Technology that enables employee monitoring may be unaffordable for smaller organizations, given the average small business owner's financial means.	Review logs on a regular basis in order to detect and respond to possible malicious behavior. Consider implementing open source solutions that involve lower overall costs.

Cybersecurity Best Practice	Problems or Potential Problems for Implementing Best Practices	Recommendations
CSG best practice 18	Given India's internet penetration rate of only 11%, the highest internet usage may occur in highly populated areas or business centers. Most adults use their computer at work for personal purposes, as well as work.	Offer security awareness training that includes social media guidelines. In social media training, be sure to include social engineering awareness and the dangers of publishing too much information online.
	Small businesses in India receive some of the highest percentages of email riddled with viruses and other cyberattacks [Symantec 2013].	Deploy up-to-date antivirus software at both the network and endpoint level to mitigate malware risks. Implement content filtering and intrusion detection systems on all corporate networks.
CSG best practice 9	India's requirement that all encryption keys larger than 40 bits be placed on file with the government can create risks for organizations attempting to secure their data in the cloud, particularly if it is hosted in India. Data hosted in the cloud is then under the care of a third party. Malicious insiders who work for the cloud services provider (CSP) might be able to access the data stored in the cloud due to the weak cryptography that may be implemented. If the company uses stronger keys and stored them with the Department of Telecommunications, malicious insiders working in the Department might be able to obtain the encryption keys. To be successful, this scenario requires collusion of a malicious insider at either the organization or hosting provider (unless the government employee had access to government-stored data as well). However, the current reputation for corruption within the government indicates that is possible.	None at this time

Cybersecurity Best Practice	Problems or Potential Problems for Implementing Best Practices	Recommendations
India - Prevalent culture and subcultures		
CSG best practice 16	The culture is heterogeneous, with strong regional cultural affiliations.	Consider the various cultural contexts in which your organization operates including but not limited to national, regional, industrial, and professional when developing a formalized insider threat program. Consider the organizational culture when developing the program to increase the chance of its adoption and institutionalization.
	India is a high-context culture where cultural knowledge is implicit, and contextually bound non-verbal aspects of communication are important.	Consider the linguistic diversity, modes of communication and high-to-low-context aspects of communication that might be present in those covered by the program.
	India is a collectivistic culture where the good of the group is favored over that of the individual.	Consider the collectivistic nature of India to increase the chances of having suspicious behavior reported. Individuals who have strong collectivistic tendencies may be hesitant to report suspicious behaviors of co-workers. Training materials should include examples that stress benefits to the larger group, society, etc.
	Trust and loyalty are important characteristics of collectivistic cultures including that between employees, and between the employer and its employees.	Consider employees' trust and loyalty when developing, deploying, and communicating about insider threat programs.
CSG best practice 13	Monitoring and controlling remote access from all end points, including mobile devices, may be perceived or interpreted by some employees as the employer's lack of trust or loyalty.	Point out to your employees that monitoring and controlling remote access from all end points is beneficial to the group as well as the organization. Offer group-level incentives that could influence compliance, acceptance, behaviors, and actions associated with monitoring and control.
	Employees who think their employer has operated outside the Indian collectivistic norm could feel less loyalty to the organization and take negative action against it.	Point out to your employees that monitoring and controlling remote access from all end points is beneficial to the group as well as the organization. Offer group-level incentives that could influence compliance, acceptance, behaviors, and actions associated with monitoring and control.

Cybersecurity Best Practice	Problems or Potential Problems for Implementing Best Practices	Recommendations
CSG best practice 4	Periodic reinvestigations, monitoring, and responding to suspicious or disruptive behavior might be viewed as an employer's lack of trust or loyalty.	Ensure employees understand the benefits that these practices provide to both the group and the organization. After identifying suspicious or disruptive behavior, show how the action impacted the larger group, without naming the individual involved.
CSG best practice 18	India is a collectivistic culture in which the good of the group is favored over that of the individual. However, the country also has great cultural diversity, so some subcultures may be very individualistic.	Consider showing employees examples of how violating social media policies and practices could impact the good of the group as well as the individual. To increase compliance and institutionalization of social media policies and procedures, consider the organizational culture—and the various cultures represented in the workforce—when developing policies, procedures, and training materials.
	India has great linguistic diversity, which can make effective communication to employees challenging.	Ensure effective communication of social media policies, procedures, and education by making sure the language and modes of communication consider the linguistic diversity and the high-low context aspects of communication that might be present in those covered by the program.
CSG best practice 9	Cloud services may be provided by organizations that reside in countries with cultures different than India's.	Consider the high-low context continuum, and various individualistic and collectivistic characteristics when developing your organization's policies, practices, and training materials.
India - Law enforcement		
CSG best practice 16	Organizations could potentially lose access to important data needed to function and make money when whole computer systems are confiscated during a police investigation. That possible confiscation could cause organizations to avoid involving law enforcement, where legal to do so.	Make a formal response plan part of your insider threat program. In that plan, include how and when to engage with law enforcement for cyber-related insider threat incidents. Make sure your insider threat program considers the fact that there are few cybercrime investigation units in India's law enforcement structure. Consider and develop robust non-law-enforcement options for preventing, detecting, and responding to threats from malicious insiders. Consider engaging with private consultants or businesses that specialize in cyber forensic incident response, at least for the initial part of the response plan, rather than directly involving local law enforcement.

Cybersecurity Best Practice	Problems or Potential Problems for Implementing Best Practices	Recommendations
CSG best practice 13	Although the IT Act addresses many cybercrimes, it does not cover the majority of crimes committed through mobile phones.	Limit access to data or functions that could inflict major damage to the company to employees physically located inside the workplace. Limit remote system administrator access to the smallest group practicable, or prohibit it altogether. Carefully consider and develop robust policies to control remote access, since law enforcement in India is not likely to be a viable deterrent.
	Remote cyberattacks that are illegal in India (other than those orchestrated through mobile phones) are unlikely to be investigated or brought to trial due to India's low number of cybercrime investigation units.	Companies should consider either developing indigenous cybersecurity response capabilities or establishing an existing relationship with a private consultant or cyber forensic business that can help your organization resolve observed suspicious cyber activity. This might also include contracts and SLAs with outside legal services that specialize in cybercrime.
CSG best practice 4	There is no evidence of a policy telling employers to avoid asking applicants about convictions on job applications unless those convictions are job related and required by the business.	Use records of convictions rather than arrests when making hiring decisions.
	Indian law enforcement has not been widely effective when it comes to cybersecurity crimes, so the absence of conviction records is probably not a reliable indicator during the hiring process.	Establish an existing relationship with a private consultant or cyber forensic business that can help your organization resolve observed suspicious cyber activity.
	Since there are only 21 law enforcement cybercrime investigation units in the entire country, relying on law enforcement may not be a viable strategy for investigating suspicious cyber behavior.	Companies should consider either developing indigenous cybersecurity response capabilities or establishing an existing relationship with a private consultant or cyber forensic business that can help your organization resolve observed suspicious cyber activity. This might also include contracts and SLAs with outside legal services that specialize in cybercrime.

Cybersecurity Best Practice	Problems or Potential Problems for Implementing Best Practices	Recommendations
CSG best practice 18	Social media use can lead to social engineering attacks on employees and the organization.	Take into account the recent rise of cybercrime in India and consider applying extra effort to train employees to avoid common social media mistakes that empower social engineering attacks. Consider contacting your supporting cybercrime investigative unit and establish frequent liaison to stay current on new cybercrime trends in social media and get help when law enforcement response is needed.
CSG best practice 9	Although the IT Act strengthened Indian law enforcement's ability to handle cybercrimes, the law is not necessarily understood or applied equally throughout the country.	Consider which law enforcement jurisdictions will apply to your organization's cloud services business partners. Ensure that your organization's cloud service contracts clearly articulate all your expected cybersecurity standards and do not rely on provisions of the IT Act being sufficiently understood or applied.
	India's law enforcement is unlikely to uphold those service level agreement (SLA) contracts (even if standards are fully articulated), because there are so few cybersecurity-savvy law enforcement personnel to cover the large Indian population.	Consider alternative methods of enforcing those SLA contracts that could carry an incentive or indicate a clear risk—for example, ask a respected international standards body to perform unannounced checks/audits (if a company fails, it could face great financial loss).
India - Corruption		
CSG best practice 16	Public sector corruption in India is considered quite high when compared to other countries.	Include mechanisms of checks and balances to ensure that bribery and other corruption have not influenced the organization's ability to prevent, detect, or respond to legitimate insider threats.
	Corruption is a daily struggle for Indian citizens, wherein, 54% of households say they have had to pay bribes to receive basic government services.	Especially within the government, be vigilant in detecting and responding to bribery, which is widely considered to be an integral way of getting things done.
CSG best practice 13	Software piracy is a widespread problem and could introduce an unmanaged cybersecurity risk. Organizations may be unable to effectively monitor and secure end points if pirated software is used by employees, due to the increasing proliferation of mobile platform malware.	Implement frequent and widespread training and awareness programs to all employees on the dangers and risks of using pirated software, both on company assets and as an attack platform from employees' personal computers and devices. Consider providing incentives to employees that report pirated software that is discovered on company networks and implement sanctions on those employees that install the pirated software.

Cybersecurity Best Practice	Problems or Potential Problems for Implementing Best Practices	Recommendations
CSG best practice 4	There is a high level of occupational fraud by employees, through which Indian businesses lose about 4,000 crore (approximately $689M USD) each year. This trend appears to be even more prevalent in the IT industry.	Consider exercising extra diligence when verifying employment histories and purported education and skills.
CSG best practice 18	Government anti-corruption efforts are largely ineffective, but a recent grassroots anti-corruption movement used social media to expose allegations of corruption.	Consider how social media could help you either prevent or detect organizational corruption that could affect your organization's cybersecurity posture.
CSG best practice 9	The high level of corruption in India, specifically manifested through bribery, has been inculcated in the Indian business world.	Strictly enforce supply chain management, assess suppliers, and ensure transparency in overall information security and management practices. Consider how corruption could impact your organization's cloud services. Include provisions in your cloud services contracts for requesting security audits of your organization's trusted business partners. These audits could be both scheduled and spontaneous in order to strengthen confidence in their results.

3 Germany

In this section, we describe Germany in terms of five factors: information technology (IT) systems, relevant laws, corruption, law enforcement, and culture and subcultures.

3.1 Country Profile

Germany is a highly developed nation of 82 million people, with many cybersecurity and privacy regulations that are strongly enforced. The internet is used by 82% of the population, and 99% are covered by a mobile network signal [World Economic Forum 2013]. EU cybersecurity and privacy laws apply there. Germany has an advanced cybersecurity capability and a long history of supporting IT innovation. In 1986, Germany established a federal office for cybersecurity (called the BSI) to formulate the degree of security required to implement IT [Federal Office for Information Security 2013b]. For its efforts in data protection, the German federal government has been awarded the Cyber Award International by Symantec [Croft 2011]. Germany is the United States' fifth largest trade partner, with imports and exports totaling approximately $147.5 billion per year. Below, we detail Germany's technological profile, relevant laws, law enforcement profile, corruption profile, and prevalent culture and subcultures.

3.1.1 Technological Profile

The western and eastern parts of Germany vary greatly in their communications (and other) infrastructure and technologies [CIA 2013b], due to European conflicts, World Wars I and II, and the Cold War. As of 2001, Germany had 51.8 million landlines and 108.7 million wireless cellphone lines [CIA 2013b]. A total of 2.1 million tablet computers were sold in Germany in 2011; by 2012, the number increased by 29% to 2.7 million [Bitkom 2013]. 40% of Germans aged 14 and above own a smartphone. Two-thirds of Germans under the age of 30 own a smartphone [Bitkom 2013]. Germany has a technologically advanced telecommunications system, including some integrated legacy systems in the eastern part of the country [CIA 2013b]. By 2016, the Bitkom industry association estimates that 10% of IT spending in Germany will be for cloud computing [Heng 2012].

The telecommunications infrastructure consists of an extensive system of automatic telephone exchanges connected by networks of fiber-optic cable, coaxial cable, microwave radio relay, and domestic satellite systems [CIA 2013b].

Cellphone service is increasing and includes roaming service to many foreign countries [CIA 2013b]. In December of 2010, Germany began to roll out the long-term evolution (LTE) protocol, which provides increased bit rates compared to 3G services [izmf.de 2013]. In 2010, 360 MHz of spectrum were auctioned for wireless network access, in order to meet spectrum and performance needs of mobile wireless applications [Federal Ministry of Economics and Technology 2010]. That addition doubled the range available for use in Germany [Federal Ministry of Economics and Technology 2010]. Germany has both 3G and LTE services [World Time Zone 2013], using the GSM mobile wireless communication protocol [The German Way 2013]. In December 2012, smartphone operating systems in Germany were as follows [Singh 2012]:

- 75% Android

- 20% Apple IOS
- less than 5% Blackberry
- less than 5% Microsoft Windows

In 2011, 16% of German small and medium-size businesses used cloud computing; this number grew to approximately 25% in 2012 [Heng 2012].

As of 2010, 82% of households and 97% of enterprises within Germany had access to the internet [ENISA 2011b]. Germany is the second most populous country in Europe with a population of approximately 81 million people as of 2013 [CIA 2013b]. 65% of data traffic is used by 10% of Deutsche Telekom subscribers [Heng 2012]. As of 2012 in Germany, there were approximately 20 million internet hosts—machines or applications that are connected to the internet and have IP addresses—and 65 million internet users [Federal Ministry of Economics and Technology 2010]. Household internet access within Germany is higher than the European average [ENISA 2011b]. 9% of the German population reported that they have security concerns related to performing activities via the internet such as banking and shopping, according to a 2010 study [ENISA 2011b]. As of 2012, 47% of Germans used online banking, which resulted from an increase in better smartphones, affordable data plans, and new banking apps [Deutsche Bank Research 2011]. This resulted in an 80% satisfaction rate for online banking among Germans [Deutsche Bank Research 2011]. By the end of 2010, Germany lost an estimated 17 million euros from approximately 5,000 phishing attacks [Fuerstenau 2010]. 72% of the German population use and maintain updated IT security software to protect computers and data [ENISA 2011b]. 39% of internet users in Germany are said to encrypt their internet traffic, compared to 18% in the United States [Karganis 2013]. 31% of German enterprises have a formally defined Information and Communication Technology (ICT) security policy [ENISA 2011b]. The German Federal Ministry of the Interior (BMI) has the responsibility of guaranteeing the internal security of the country [Federal Ministry of the Interior 2009]. This includes information security policy, protection of critical information infrastructures, and e-government.

Germany ranked 16th out of 142 countries worldwide, with a score of 5.32 out of 7.0 on the 2012 Networked Readiness Index (NRI) [World Economic Forum 2012]. The NRI is a system that ranks economies based on their capacity to exploit the opportunities offered by ICTs for enhanced competitiveness and well-being [World Economic Forum 2013]. The readiness sub-index ranks Germany 14th for infrastructure and digital content, 38th for affordability, and 20th for skills [World Economic Forum 2012]. The usage sub-index ranks Germany 14th for individual usage, 6th for business usage, and 30th for government usage [World Economic Forum 2012]. That sub-index uses indicators such as mobile phone subscriptions, individual use of the internet, households with a personal computer, households with internet access, fixed and mobile broadband subscriptions, and the use of social networks [World Economic Forum 2012]. Global trade of ICT products has doubled, from $2.2B USD to $4B USD as of 2008 [Federal Ministry of Economics and Technology 2010]. The highest growth in ICT exports has been IT services: from $70B USD in 1996 to $325B USD as of 2008—an increase of approximately 14% per year [Federal Ministry of Economics and Technology 2010]. Germany has ranked third in the EU regarding the amount of investments in IT infrastructure [Heng 2010].

Foreign countries are known to monitor European traffic [Spiegel 2013a]. Twelve years ago, a European Parliament committee stated that all communication (email, telephone, and fax) were

monitored by the American, British, Canadian, and Australian intelligence services. Steps were taken to regulate such monitoring, but those came to a halt after the 9/11 attacks by airplanes on the New York City twin towers [Spiegel 2013a]. Recently, information has been disclosed by Edward Snowden about an alleged communication-monitoring partnership among the U.S. NSA, the German government—specifically the Federal Intelligence Service (BND)—and other European countries. This partnership focuses on the traffic that goes through Germany's financial center, Frankfurt, where a majority of traffic from Eastern Europe, Central Asia, and the Middle East converge, allowing for easy access to data communications streams and monitoring for potential threats [Spiegel 2013a].

In 2010, a German court ruled that national laws instated to meet the EU Data Retention Directive were unconstitutional [Fuerstenau 2010].

The BSI runs CERT-Bund, the federal computer security incident response team in Germany [Federal Office for Information Security 2013a]. CERT-Bund is the central point of contact for preventing and reacting to incidents related to computer security [izmf.de 2013]. In order to prevent damage, CERT-Bund publishes recommendations and preventative measures; exposes and provides mitigation measures for hardware and software product vulnerabilities; and supports public efforts in responding to IT incidents [izmf.de 2013]. CERT-Bund offers services primarily to federal authorities, including 24-hour on-call duty, analysis of incident reports, operation of warning and information services, and alerting the federal administration in case of danger [izmf.de 2013].

3.1.2 Relevant Laws

A recent study of German cybercrime found that malicious insiders caused some of the most costly cybercrimes and insider crimes take an average of 42 days to contain (compared to the United States, where the average is 57 days) [Ponemon 2012b, Ponemon 2012a]. Germany's cybercrime and privacy legal framework is implicated in many aspects of addressing insider threats. The framework is considered "comprehensive" by the BSA, but there is uncertainty about application of the laws given the 17 data protection authorities' varied implementations [BSA 2013a].

Germany has signed and ratified the Budapest Convention on Cybercrime, as well as the Additional Protocol to the Convention on Cybercrime [COE 2004, COE 2013]. Over 40 nations, including the United States, are signatories of the Convention, which entered into force in Germany in 2009 [COE 2004]. The German criminal code was amended to criminalize activities including illegal access to computer systems, data tampering, computer sabotage, and computer-related fraud [COE 2009]. In addition, the German Federal Ministry of the Interior has proposed a notification requirement for cybersecurity breaches. Data breach notification is already required for significant breaches of sensitive data [German Federal States 2010, Hunton & Williams 2011a].

While there are state-level regulations, Germany's primary privacy law is the Federal Personal Data Protection Act of 2001. Section 32 of the Act discusses data collection for employment purposes and allows for processing "where necessary for hiring decisions or, after hiring, for carrying out or terminating the employment contract" [German Federal States 2010]. Section 32 also limits the collection and use of employees' personal data during investigations only if there is documented suspicion, the collection is necessary, and the employee does not have an overriding interest in prohibiting collection. In addition, the Federal Commissioner for Data Protection and Free-

dom of Information has discussed the legalities of an employer monitoring its employees' internet use and emails [Federal Commissioner for Data Protection and Freedom of Information 2013]. The Commissioner notes

> *"a complete monitoring of the e-mail traffic or of the surfing behavior is not admissible because this would involve the permanent surveillance of the employee. Such an automated complete monitoring is a severe intrusion into the employees' personal right and therefore not permissible. However, the employer is entitled to carry out a random and contemporary analysis of the log data. In this connection, the procedure has to be made as transparent as possible" [Federal Commissioner for Data Protection and Freedom of Information 2013].*

Video surveillance is also limited, requiring more than a general suspicion of wrongdoing, and ideally should be carried out openly [Federal Commissioner for Data Protection and Freedom of Information 2013]. Draft laws have been proposed specifically around employee data protection; however we could not find further information about it [ENISA 2011b]. An organization may hold many other assets besides personal information, such as patents, trade secrets, and geolocation or biometric data, and a variety of legal frameworks may be present to regulate what can be collected and how it can be used or stored. While the scope of this report does not allow for a detailed discussion of all these regulations, recent examples of such data and regulations include national-security-related telecommunications information [Spiegel 2013b].

Because a robust insider threat program includes background screening, labor laws may be applicable. German's Federal Anti-Discrimination Agency (FADA) enforces the General Equal Treatment Act, which prohibits employment discrimination based on ethnic origin, gender, disability, religion, belief, age, and sexual orientation. The FADA has even piloted an anonymous application process that initially excludes an employer from viewing an applicant's "name, age, gender, and family status" [Lüders 2013]. Other labor laws may also be implicated. For example, absences from work may be considered a potential indicator related to insider threats, but in Germany, sick days may not be tracked, thus limiting this potential indicator [Roberts 2008].

Finally, there are also some laws surrounding whistle-blowers in Germany, which could be of interest to organizations setting up insider threat programs. While German corporate law does not require a whistle-blower program, it does require certain measures that, when taken with other considerations, have led to "enhanced reflections on whistle-blowing systems within the German economy" [Strack 2011]. Other instruments that have influenced whistle-blowing protections include the United Nations Convention Against Corruption and the Council of Europe conventions against corruption [Strack 2011]. When designing protections for whistle-blowers, an organization must consider Germany's data protection laws; however, the Article 29 working group of the EU's Data Privacy Directive (DPD) has developed a decision that helps make the protections compatible with data privacy [Strack 2011]. This includes the recommendation of

> *"accepting anonymous reports (i.e., also information) only in exceptional cases. Anonymity contradicts the principle of transparency, and—compared with identifying names—promotes misuse and denunciations" [Aguilar 2007].*

While whistle-blowing to law enforcement should be a right protected from retaliation, recent case law has made the process burdensome and does not protect the employee from retaliation [Strack 2011].

3.1.3 Law Enforcement Profile

Many law enforcement agencies, as well as agencies that help them, are used in the fight against cybercrime in Germany. These agencies include the National Cyber Defense Center (NCAZ) and the National Cyber Security Committee [Kington 2013]. The latter involves the chancellery, as well as industry representatives from state and other ministries, and was instituted to help evaluate the whole spectrum of cybersecurity policy [Kington 2013]. The NCAZ is multifaceted and includes the police, civil defense organizations, the military, the secret service, and security organizations [Kington 2013]. The NCAZ works closely with the BND [ENISA 2011b].

Other agencies that operate in the law enforcement arena in Germany include the Computer Network Operations Team that has the capability to take offensive action in regards to cybersecurity issues; however, it only does so with proper permissions given by the German parliament [Kington 2013]. It is part of the Bundeswehr or Federal Defense. In addition, the Bundeskriminalamt (BKA) [bka.de 2013], also known as the Federal Criminal Police Office, is actively involved in deterring cybercrime [statewatch 2013].

The Federal Office for Information Security (the BSI) is similar to the Computer Security Division (CSD) of the Information Technology Laboratory in the U.S. National Institute of Standards and Technology (NIST) [Federal Office for Information Security 2013a]. It is tasked with providing communication security and the management of computers for the German government. In 2009, the Act to Strengthen the Security of Federal Information Technology was passed [Federal Office for Information Security 2013a]. CERT-Bund operates under the BSI [Federal Office for Information Security 2013c] and runs Germany's national IT Situation Centre that provides an "umbrella strategy for IT security" [Federal Office for Information Security 2013c].

Out of the government agencies listed above, the BKA appears to be most directly involved in the cybercrime arena. The BKA, which is considered to be the equivalent of the U.S. Federal Bureau of Investigation [Gallagher 2012], is involved in many aspects of cybersecurity law enforcement, including working to coordinate criminal investigation authorities within both state and federal police forces. Once that occurs, the BKA also coordinates with foreign investigative authorities. It manages the INPOL database, or Police Information System in Germany, which includes information on all important crimes and criminals [statewatch 2013]. Furthermore, according to the BKA website, it is an agency that monitors the internet for criminal offenses related to data networks and threats against information technology that may include hacking, computer sabotage, and abuse of telecommunications means [bka.de 2013]. Once detected, infractions are passed onto the police for follow-up [bka.de 2013]. According to German Vice President Jurgen Maurer, 600,000 cases of cybercrime were registered with the BKA in 2011 [Fuerstenau 2013].

The BKA has its own surveillance software and is continually working to further develop its telecommunications surveillance software [Borchers 2013]. The latter becomes an issue, particularly for the German Federal Privacy Commissioner because he says the boundaries may become blurred when attempting to ensure that the software is not used in a way that could infringe on people's constitutionally protected privacy rights [Borchers 2013].

The *Cyber Security Strategy for Germany* says that the efficiency of various entities (including the BSI, law enforcement agencies, and the private sector) in contending with cybercrime and combating sabotage and espionage must be strengthened [ENISA 2011a, p. 6]. The National

Cyber Response Center was developed to address operational concerns that occur between the state authorities and improve the measures taken to manage IT incidents [ENISA 2011a]. Likewise, officials determined that to face global cybercrime effectively, a great effort must be put forth to "achieve global harmonization in criminal law based on the Council of Europe Cyber Crime Convention" [ENISA 2011a].

The German government—in particular, the Left Party—questions how working with the EU's cybersecurity team towards a security strategy for the internet will impact German law enforcement entities and potentially cause blurring between the distinct intelligence, military, and law enforcement agencies [BBC 2011].

Data protection is an important and often controversial topic in Germany. According to the German Federal Data Protection Act (FDPA), its role is "to protect the individual so that he is not disadvantaged in his personal rights through the handling of his personal data." It allows for a "right to information self-determination," which allows Germans to determine if they want their information shared—with the exception of cases that are deemed possible terrorist scenarios. That exception resulted from the German court's decision in 2008 when it determined that domestic security services were permitted to be used to monitor the computer activity of those suspected of terrorism or crimes [Reuters 2008, Federal Office for Information Security 2013d]. There must be supporting evidence prior to beginning the monitoring, and a judge must approve the surveillance [Reuters 2008]. A ruling by the Federal Constitutional Court stated that, "It is part of the constitutional identity of the Federal Republic of Germany that citizens' enjoyment of freedom may not be totally recorded and registered" [German Federal Ministry of Justice 2013]. Law enforcement agencies must be careful to fully abide by the FDPA.

Citizens in a democratic society like Germany influence the scope of law enforcement. Related to that, 69% of Germans felt that their internet activity should not be monitored in order to prevent and/or detect infractions of the law (cybersecurity and other laws). Likewise, Germans supported "government censorship" at a rate of 52% of those questioned [Karganis 2013].

Germany is the first country to implement computer network systems crimes such as data forgery, information on spying, and computer sabotage into its Criminal Code [Wang 2011]. A number of high-profile hackers have been prosecuted for such things as stealing unpublished songs and attempting to blackmail the artists, and one hacker was incarcerated for a DDoS extortion scam against online betting sites for the World Cup [NCC Group 2011]. In addition, in May of 2013, Germany arrested two Dutch citizens who were involved in a cyber bank heist [Hübner 2013].

One example of the way law enforcement in Germany has taken action is the bust by the Internet Crime Unit of the German Landeskriminalamt-Baden Wurttemberg (LKA). During that bust, the German State Criminal Police sent agents in to shut down a hacking underground market operation that allowed cyber criminals to share information-stealing tools and information about things such as cloning credit cards [Constantin 2009]. The raid involved taking two computers with high-capacity storage [Constantin 2009]. In another case, an 18-month police investigation led to arrests of 10 international phishing suspects [Gaudin 2007]. The cyber criminals' target was two online banks, and during the investigation, the police seized computers in order to gain further evidence [Gaudin 2007].

Germany has a "hacker clause" that essentially forbids anyone from selling and distributing hacking tools [Higgins 2011]. Many researchers are being threatened with legal action for exposing software vulnerabilities [Higgins 2011]. While there appears to be no international hacker conferences (such as BSides [Security B-Sides 2013] or Black Hat [blackhat.com 2013] that currently take place in Germany), a Chaos Computer Club (CCC) has been active for over 20 years [CCC 2013]. The CCC is a Germany-based group that supports government transparency, the right to communicate, and the freedom of information. The CCC exposed a "Bundestrojaner" (a federal Trojan) last year when it told the media that the BKA had the capabilities to record Skype calls and messenger chats [Gallagher 2012]. This surveillance program was said to even be able to use a webcam to essentially spy on the computer user [Gallagher 2012]. As in other nations, Germany's law enforcement is also being questioned regarding its surveillance usage.

In 2009, Germany was among the top five countries in terms of the number of malicious cyber activities reported: The other four were the United States, China, Brazil, and India [ITU 2012a]. Hewlett-Packard conducted a study called the "Cost of Cyber Crime" in 2012 and found that during that year "cyberattacks cost a German company an average of 4.8 million euros (U.S $6.2 million) per year" [Knigge 2013]. Another source estimates that the total cost of cybercrimes to German companies is $5,950,725 USD, a figure that is surpassed only by the United States's cost of $8,933,510 USD and is just above Japan at $5,154,447 USD [Ferran 2013]. These numbers could potentially vary due to the importance that companies may have placed on the information, and the types and frequency of the attacks that occurred [Ferran 2013]. In February of 2013, Germany was ranked the country with the third highest number of cyberattacks (780,425), behind Russia (2,402,722) and Taiwan (907,102) [GO-gulf.com 2013]. The sheer volume of cyberattacks launched on Germany annually provides law enforcement agencies with a great need to enforce the laws regarding cybersecurity. Germany ranks low on corruption, so we would expect law enforcement agencies in charge of cybersecurity issues there, such as the BKA, to follow up on these issues. Likewise, the BKA will be busy working with foreign agencies to coordinate on cybersecurity issues facing Germany, the EU, and the rest of the world.

According to Arne Schönbohm (a leading security expert in Germany) [Schönbohm 2011], due to the many bot infections that have come to Germany, including Stuxnet, the country is still under scrutiny for not investing more in cybersecurity and for having a decentralized cyber-response structure that doesn't provide efficient security. To help improve Germany's cybersecurity [Levin 2012], Schönbohm recommends greater coordination among the national computer emergency readiness teams [Schönbohm 2011].

3.1.4 Corruption Profile

Germany comprises 16 federated states [CIA 2013b] (1 free Hanseatic city—or guild city—2 city states, and 13 area states), so it may be possible to discover variations of both corruption and anti-corruption across the country. However, for the purpose of this overview, Germany will be considered as a single holistic country unless specifically noted.

Germany received a good score of 79 on the Corruption Perceptions Index for 2012, ranking it 13th out of 176 countries and territories round the world. This means that Germany is perceived to have less public sector corruption than the United States, which ranked 19th [Transparency International 2012].

Perception is important in enhancing business opportunity and investment in a country's market. However, although the worldwide perception of Germany is quite good, the German population actually views the level of corruption within the country as relatively high. Since 2003, a significant majority of the German population has indicated they believe corruption has increased or will increase: The 2010 survey showed that 70% held that view [Transparency International 2013a].

Perhaps more important than a perception index are the very strong anti-corruption controls in Germany. There are considered to be 13 anti-corruption institutions (or pillars) that, when combined, constitute a National Integrity System [Transparency International 2013c]: the legislature, the executive, the judiciary, the public sector, law enforcement, the electoral management body, the ombudsman, the supreme audit institution, the anti-corruption agency, political parties, the media, civil society, and the private sector.

The public sector is interpreted here as being the federal, state, and local administration, minus the Federal and State Ministries. It carries out public relations work to inform Germans about the significance and risks of corruption. This institution scored 71 out of 100, the weakest aspect being the education of the general public about anti-corruption mechanisms. This may be a factor in the population's perception that corruption has increased or will increase during the surveys administered for the CPI.

The population's general sense that corruption is high could possibly impact cybersecurity decision making and implementation negatively based on their perceived risk threshold.

From a private company perspective, the organizational and operational complexity, and corporate culture and internationality (or how many different countries it operates in) are factors that influence the company's inclination towards corruption. That inclination is likely to manifest itself by either the presence or absence of corruption control and prevention mechanisms [Arnold 2012].

One illuminating corruption trend in Germany that could have a significant impact on corporate cybersecurity strategy is the illegal software installations performed by mid-level business managers [Nill 2010]. Germany suffers from a significant software piracy problem. It is ranked seventh in the world in money lost through software piracy, and mid-level business managers represent one of the largest markets for software. Germany's piracy rate was 27% in 2010. Although that is still markedly lower than the 33% average in the rest of the EU, it introduces an unnecessary and unmanaged cybersecurity risk. Pirated software is often not eligible for software patches and bug fixes that can ameliorate security vulnerabilities.

Overall, Germany has a low amount of corruption in reality and has strong anti-corruption institutions, so corruption should not have much of an impact on its cybersecurity strategies and management. However, the widespread software piracy by mid-level business managers introduces some complexity and risk into cybersecurity implementation and maintenance.

3.1.5 Prevalent Culture and Subcultures in Germany

Germany, officially known as the Federal Republic of Germany, is a federal parliamentary republic located in western-central Europe. It is the largest economy in Europe and the 5th largest in the world, and is the 2nd most populated country in Europe and the 16th in the world [CIA 2013a]. Germany's labor force is the 14th largest in the world at 44,010,000 [CIA 2013a].

Germany comprises four geographic regions. In the north are the North German Plains; in the south, the Central Mountain Range; in the west, the Alpine Foothills; and in the east, the Thuringian and Bavarian Forest [Bernstein 2004]. The national language of German is Standard German. According to Ethnologue, there are 27 living languages in various stages of use [Ethnologue 2013]. Germany's linguistic diversity is ranked low as indicated by its positioning at 125 on Greenberg's language diversity index and its assigned value of 0.358, with 1 being the highest diversity and 0 being no diversity [Ethnologue 2013]. Linguistic variations in Germany are linked to regions, groups, and localities [Kelly-Holmes 2002].

Prior to 1990 and since 1949, modern-day Germany comprised two German states: the German Democratic Republic (East Germany) and the Federal Republic of Germany (West Germany). While linked by a common language, German, they were separated by border fortifications, as well as economic, political, social, and cultural differences [Bernstein 2004, Betts 2010]. On October 3, 1990, East Germany and West Germany were united after a 40-year separation.

While Germans have a common language, although with some variations, their cultural landscape can be described as heterogeneous. Cultural differences exist between them at regional, local, and group levels. According to Holmes and Boyer, some cultural and social differences (perceived and real) still exist between what were former West Germany and East Germany [Kelly-Holmes 2002, Boyer 2000]. However, to a degree, at a national level, Germany does share some broad homogeneous, culturally significant characteristics. It should be noted however, that the cultural considerations and implications put forth are broad generalizations for the purposes of this report. Because no society or culture is homogeneous, exclusions from or variations to the generalizations we posit here are to be expected.

How people communicate can provide great insights into their culture. According to Hall, when communicating, "Meaning and context are inextricably bound up with each other," and thus it is important to examine meaning and context together [Hall 1976]. To give voice and insight into the sociocultural aspects of communication, Hall created the high-low context continuum that places cultures along a dimension that ranges from high-context to low-context [Hall 1976]. Also culturally relevant is how people perceive and organize time and space. Perceptions of time and space are a sociocultural construct that influences our daily lives, how we interact with others, and how we perceive our past and future. Based on ethnographic research, Hall proposed two variant solutions of how time and space are culturally organized: monochronic time and polychronic time [Hall 1976]. The high-low context continuum and monochronic and polychronic views of time and space provide a framework for understanding culturally significant differences.

Another measure that can provide broad generalized insights into the sociocultural construct of a country is Hofstede's dimension of individualism and collectivism [Hofstede 2010]. Individualism and collectivism each represent a set of distinguishing values, and positioning on the dimension reflects either a focus of "I" (the individual) or "we" (the collective group). On a scale of 0 to 100, the most collectivistic countries are closest to 0, and those with high individualistic traits are closer to 100. Germany received an index score of 67, which places it firmly as individualistic [Hofstede 2010].

In broad general terms, Germany is a low-context, individualistic country that has a monochronic perception of time and space. Note that because German society and cultures are not homogene-

ous, the positioning of most people, groups, and possibly regions may vary on the high-low context continuum, and individualistic and collectivistic scale.

In low-context countries such as Germany, cultural knowledge is explicit. Communication occurs through explicit and direct statements both in written and spoken forms, so the listener understands the message as it was intended [Hall 1976]. Reasoning in low-context cultures tends to be linear, rational, and logical. Rules of privacy are important and observed. When resolving conflict, individualistic cultures tend toward assertive tactics and achieving justice. Research conducted on the influence of individualistic and collectivistic value orientation on decision-making processes revealed that people with individualistic values try to "prevent friction by controlling the situation through deep exploration and information gathering, are achievement-orientated, have more confidence in their personal decisions, and might be more decisive and risky than people in collectivist cultures in their decisions" [Guess 2004].

Low-context and individualistic societies display tendencies toward focusing on the good of the individual rather than the good of the group. Individualistic cultures are defined by detachment from relationships and community with individuals viewing themselves as independent from others [Guess 2004]. Relationships and trust are primarily between individuals and immediate family. Because personal ties are relatively loose, it is not uncommon for members of low-context and individualistic cultures to have many short-term relationships.

In general, Germany has a monochronic view of time. In monochronic cultures, time is viewed as structured, compartmentalized, and having the potential of being wasted [Hall 1976]. Other monochronic tendencies include an emphasis on promptness, planning, adherence to schedules and due dates, little tolerance for interruptions, and doing one thing at a time.

The CPI ranks the corruption of countries (147 in total) as perceived by the public sector and is based on views of observers from around the world. On a scale of 0 – 100, with 100 representing no corruption, Germany has been assigned a 13, placing it on the low end of the scale. The level of corruption and bribery in a country, as well as the extent of its identification and prosecution, may indicate the level of sociocultural tolerance for such practices and how engrained they are in a country's sociocultural fabric. According to Goel, Germany is not immune to corruption and bribery in both the public and private sectors. However, Goel notes that Germany has significantly strengthened its anti-corruptions laws and "is now actively investigating and prosecuting violations of anti-corruption laws," which have resulted in some of "largest monetary penalties ever imposed in any anti-corruption investigation." For additional information regarding corruption and bribery in Germany, refer to Section 3.1.4 of this report.

Because German organizations operate under the influence of low-context, individualistic, and monochronic characteristics to some extent, their culture should reflect them. However, the organizational culture and practices of countries have been known to deviate from the norm [Hall 1976]. According to Hofstede and Minkov, "In practice there is a wide range of types of employer-employee relationships within collectivistic and individualistic societies" [Hofstede 2010].

3.2 Analysis of Implementation of Five Best Practices in Germany

In this section, we analyze implementation in Germany of five best practices against insider threat. We focus on implementation issues that arise due to the nation's relevant laws, technologi-

cal profile, law enforcement profile, corruption profile, and prevalent culture and subcultures. We selected these best practices for analysis from the *Common Sense Guide to Mitigating Insider Threats*, out of its recommended 19 [Silowash 2012]:

- Practice 16: Develop a formalized insider threat program.
- Practice 13: Monitor and control remote access from all end points, including mobile devices.
- Practice 4: Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.
- Practice 18: Be especially vigilant regarding social media.
- Practice 9: Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.

3.2.1 Practice 16: Develop a formalized insider threat program.

For a summary of this best practice, see the appendix on page 64.

3.2.1.1 Effects of Germany's Technological Profile

The CSG, which offers U.S.-based advice, says that core insider threat team members need to have secure methods to communicate with each other, in a physical location or via secure electronic communication [Silowash 2012]. The presence of ICT security policies in 31% of German organizations may help those organizations provide secure communication between insider threat team members [ENISA 2011b].

The CSG also says that insider threat teams should understand who they need to coordinate with and report to [Silowash 2012]. CERT-Bund and BMI support public efforts in responding to IT incidents [Dwucet 2012]. That support can help insider threat teams prevent and react to incidents.

Germany has technologically advanced telecommunications systems [CIA 2013b] that make it fairly easy to monitor employee communications. Companies must be aware of the legality of such monitoring, which can be both a benefit and possible risk to the development of an insider threat program.

In addition, the CSG says that organizations should have policies and procedures that implement random audits of various data sources [Silowash 2012]. ICT security policies in place at 31% of German companies will help meet this goal [World Economic Forum 2012].

Coordinating with the appropriate outside organizations can help insider threat teams prepare for handling incidents. For example, they should work with BSI and CERT-Bund so they know what to look for and can respond quickly to incidents when they occur [Federal Office for Information Security 2013c].

3.2.1.2 Effects of Germany's Laws

While the FDPA allows for some collection of employee data, the Federal Commissioner for Data Protection and Freedom of Information notes that "complete monitoring" is too much of a privacy intrusion to be permissible [Federal Commissioner for Data Protection and Freedom of Information 2013]. A transparent program in which there is "random and contemporary analysis of the

log data" has been considered acceptable [Federal Commissioner for Data Protection and Freedom of Information 2013]. Other laws, such as employment regulations, may further define what information can or cannot be collected; for example, sick days may not be tracked [Roberts 2008]. Germany also outlines technical requirements for protecting personal data including access control, storage media control, memory control, user control, and input control [German Federal States 2010]. Organizations must consider these controls when collecting or analyzing personal data, some of which could be collected and/or protected as part of an insider threat program. Germany also has cybercrime laws, which may allow for the prosecution of malicious insider crime [German Federal States 2010]. Finally, as discussed in the legal summary, Germany has laws covering whistle-blower protections; however the strength of those protections has been questioned [Strack 2011]. Such laws may be of potential interest when implementing an insider threat program, because, at least in the United States, federal departments and agencies have been asked to review monitoring policies to ensure they do not target whistle-blowers [OSC 2012].

3.2.1.3 Effects of Germany's Law Enforcement Profile

The CSG states that insider threat programs "should have specific criteria and thresholds for conducting inquiries, referring to investigators [possibly law enforcement], and requesting prosecution" [Silowash 2012]. In Germany, the National Cyber Security Committee helps to evaluate the whole spectrum of cybersecurity policy, including that used for the incident response plan [Kington 2013]. An organization may look to that Committee for advice on how to come up with thresholds and criteria regarding cybersecurity-related policies, since the Committee is made up of law enforcement officials [Center for Strategic and International Studies 2011]. In addition to the National Cyber Security Committee, Germany's computer security incident response team, CERT-Bund, may further help organizations determine thresholds and criteria, and currently does so for many German federal agencies [Federal Office for Information Security 2013c].

Organizations should implement an established incident response plan that aims to address any incidents that occur as a result of insider attacks. That plan should include information on how and when to contact cybersecurity law enforcement agencies such as the BKA, which is involved in many aspects of cybersecurity law enforcement, including working to coordinate criminal investigation authorities within both state and federal police forces. The BKA also coordinates with foreign investigative authorities.

3.2.1.4 Effects of Germany's Corruption Profile

Germany has a strong privacy and civil liberties view concerning workers' rights and privileges, as discussed in Section 3.1.2. This may result in an insider threat program being perceived negatively from the German workforce's perspective. It may be better to describe a formal insider threat program as an example of German commitment to anti-corruption [Transparency International 2013c].

In several high-profile cases of corruption, companies have used a form of management called co-determination. Charges were filed against these companies for bribery, illicit sex, and company-sponsored shopping sprees used to influence worker representatives [Landler 2008]. And in 2010, the Transparency International Global Corruption Barometer showed that 70% of Germans believed that corruption has increased or will increase [Transparency International 2013a].

A formal insider threat program that is described, in part, as supporting the private sector institution of the National Integrity System [Transparency International 2013c] might be viewed more favorably by employees.

3.2.1.5 Effects of Germany's Prevalent Culture and Subcultures

While Germans have a common language, although with variations, organizations operate in a heterogeneous cultural landscape [Ethnologue 2013, Kelly-Holmes 2002]. When developing a formal insider threat program, organizations should consider the various cultural contexts in which they operate including but not limited to national, regional, industrial, and professional. The culture of the organization, and its values and beliefs such as "we are the best at…" or "we provide outstanding products and services" are also relevant. Beliefs and ideas about an organization are shared assumptions of reality used to rationalize behavior. To increase the chance of a formal insider threat program being adopted and institutionalized, an organization should consider its culture when developing the program.

Because Germany is a low-context and individualistic country [Hofstede 2010], German organizations should consider using direct and explicit statements when developing policies, processes, and procedures associated with a formalized insider threat program. Because German cultures are not homogeneous, they might encompass people, groups, and possibly regions whose positioning may vary on the high-low context continuum, and individualistic and collectivistic scale. Thus, an organization should consider the cultural composition of its workforce when developing a formalized insider threat program. When developing guidelines and scenarios for insider threat programs, organizations operating in Germany should remember that individualistic cultures generally display tendencies toward focusing on the good of the individual rather than the good of the group: Considering that individualistic nature might increase the chances of employees reporting suspicious behavior. In addition, organizations should communicate their insider threat program in an explicit and direct way, and publicize the benefits the program will provide to employees.

3.2.2 Practice 13: Monitor and control remote access from all end points, including mobile devices.

For a summary of this best practice, see the appendix on page 64.

3.2.2.1 Effects of Germany's Technological Profile

Organizations operating in Germany and those that have agreements with organizations in Germany need to be aware of the laws governing monitoring, especially if personally owned devices are used. Email, logs, and data generated by the employee during the course of employment may be protected, and certain conditions may need to be met in order to review that information.

Smartphones are becoming more commonplace in Germany: Two-thirds of its population under the age of 30 own one [Bitkom 2013]. Smartphones present a way for sensitive information to exit the organization using phone features such as email (personal or corporate), cameras, voice recording, and online storage. Mobile phone usage in an organization should be carefully controlled and the risks weighed before their use is allowed with corporate information systems.

3.2.2.2 Effects of Germany's Laws

One recent movement that may affect this practice is "bring your own device" (BYOD), in which employees bring their own mobile devices, laptops, or other such devices and use them at work. Such practices may have implications with respect to an employer's ability to monitor the devices. The German Federal Office for Information Security has discussed BYOD, noting issues "ranging from data protection concerns to software licensing and issues of civil liability" [Hunton & Williams 2013a]. The Office suggests specific practices including developing user agreements and separating private use from work use [Hunton & Williams 2013a]. As we noted in Section 3.1.2, complete monitoring is considered a severe intrusion into an employee's personal rights and is unlikely to be allowed [Federal Commissioner for Data Protection and Freedom of Information 2013].

3.2.2.3 Effects of Germany's Law Enforcement Profile

Organizations need to build numerous levels of defense against a remote or off-site attack. Likewise, organizations should include mobile devices in their risk assessments due to specific features available on these devices such as remote access, cameras, massive storage capabilities, and microphones that could be used for data exfiltration. The German National Cyber Security Committee, as well as CERT-Bund, could help organizations develop appropriate defenses against remote attacks, particularly in light of Germany's stringent data protection regulations [Kington 2013, German Federal Ministry of Justice 2013, Federal Office for Information Security 2013d].

3.2.2.4 Effects of Germany's Corruption Profile

Although the software piracy rate in Germany was only 27% in 2010 (which is markedly lower than the EU's 33% average), the predominant sector involved in the piracy was German mid-level managers [Nill 2010]. As we discussed in Section 3.1.4, pirated software could introduce an unmanaged cybersecurity risk especially because it is often not eligible for software patches and bug fixes that can ameliorate known security vulnerabilities.

3.2.2.5 Effects of Germany's Prevalent Culture and Subcultures

Rules of privacy are important and observed in individualistic countries such as Germany. Germans were outraged when news of electronic surveillance operations was announced. One of the responses by German officials was to publicly cancel the 1968-69 "spy" pact with the United States. German Foreign Minister Guido Westerwelle said in a statement, "The cancellation of the administrative agreements, which we have pushed for in recent weeks, is a necessary and proper consequence of the recent debate about protecting personal privacy" [BBC 2013]. Spiegel Online International has suggested a greater cooperation between German and U.S. intelligence agencies than has been publicly acknowledged. Regardless of whether it is true, the publicity that suggestion received could lead to a heightened awareness of an individual's right to privacy [Spiegel 2013c].

Because Germany is individualistic, employees there may view monitoring and controlling remote access from all ends points, including mobile devices, as an intrusion to an employee's personal rights that infringes on rules of privacy [Spiegel 2013c]. Given the heightened awareness of monitoring in Germany, that perception could potentially impact employees' loyalty and therefore their actions. For example, they might try to work around any controls or even resign from their

jobs. Organizations may consider publicizing the monitoring and controlling of remote access from all end points, including mobile devices, as a practice that is not only beneficial to the organization but also to each individual in it. Individual-level incentives may influence the compliance, acceptance, behaviors, and actions associated with that monitoring and control.

3.2.3 Practice 4: Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.

For a summary of this best practice, see the appendix on page 63.

3.2.3.1 Effects of Germany's Technological Profile

Organizations operating in Germany should consider implementing additional monitoring capabilities to detect and prevent malicious insiders. Organizations may find it beneficial to implement additional monitoring (within legal authority) during probationary periods or with positions that have high turnover rates. The CSG recommends that organizations review logs on a regular basis to detect and respond to possible malicious behavior [Silowash 2012]. Since 31% of German enterprises have formally defined ICT security policies [ENISA 2011b], these enterprises may be able to leverage existing policies to implement additional monitoring. Furthermore, organizations with security policies in place may have technology already implemented in their organization that can help implement monitoring capabilities. For instance, organizations that already have an audit log system or security information and event management (SIEM) system in place may find it easier to implement additional monitoring by changing audit policies and adding to system storage capabilities. Even the 69% of organizations in Germany without a formal ICT security policy might have a SIEM system or audit log system in place; security systems like these may be more affordable in Germany—a developed country with a relatively high standard of living (compared to the majority of other countries in the world)—than they are in less-developed countries. Organizations that cannot afford commercial products could implement open source solutions that involve lower overall costs.

3.2.3.2 Effects of Germany's Laws

Germany has specific regulations with respect to background checks. For example, third parties may not access criminal records; rather, the applicant must initiate the search [Krell 2013]. In addition, at least one source indicates employment contracts may take months to terminate, which is a potential consideration when developing a response plan for addressing suspicious or disruptive behavior [Krell 2013]. Germany also has discrimination prohibitions that appear to be along the same lines as those in the United States [Lüders 2013].

3.2.3.3 Effects of Germany's Law Enforcement Profile

To implement this best practice, the CSG recommends that organizations conduct background checks during the hiring process in order to evaluate if there are any previous criminal convictions, credit problems, or issues with past employment [Silowash 2012]. All of this should be done with consideration to legal requirements. Depending on the current German law, organizations might be able to consult the BKA regarding past convictions of potential employees [bka.de 2013]. The BKA also monitors the internet for criminal offenses that are related to data networks and threats made against IT, including hacking, computer sabotage, and abuse of telecommunica-

tions equipment [bka.de 2013]. If information is obtained through legal means, the BKA might be able to provide it to the appropriate agencies conducting the background checks.

Organizations must also be vigilant about enforcing workplace policies and procedures for all employees and have a consistent method of investigating and responding to rule violations. Many of these policies are cybersecurity-related and may be referred to the National Cyber Security Committee [Kington 2013], CERT-Bund, an organization coordinating with the BSI, or the Federal Office for Information Security [Federal Office for Information Security 2013d]. Enforcement failure could embolden insiders to commit further violations.

3.2.3.4 Effects of Germany's Corruption Profile

Germany does not appear to have any significant corruption that would negatively affect this best practice.

3.2.3.5 Effects of Germany's Prevalent Culture and Subcultures

Rules of privacy are important and observed in individualistic countries such as Germany [Hofstede 2013]. For example, to address data privacy concerns, some organizations, such as the German lawyers' association, are encrypting data placed in the cloud by cloud service providers (CSPs) and not giving vendors access to the encryption key [Abboud 2013]. Another example is the suggestion made by lawmakers in the European parliament that would allow cloud computing customers to "opt out of their data being stored in the United States" and to require supervision of the transfer of personal data to overseas CSPs [Abboud 2013]. When background checks are performed as part of the hiring process and periodic reinvestigations that follow organizational policies and privacy rules and laws, the effect on the individual employee should be minimal. Organizations may further reduce the effect by ensuring that all employees are informed of policies and practices associated with monitoring and responding to suspicious or disruptive behavior.

3.2.4 Practice 18: Be especially vigilant regarding social media.

For a summary of this best practice, see the appendix on page 64.

3.2.4.1 Effects of Germany's Technological Profile

Social media opens employees to possible social engineering attacks such as phishing, which has been on the rise in Germany and accounted for a loss of 17 million euros in 2010 [Fuerstenau 2010]. The fact that phishing has affected Germany in such a way is concerning: Organizations there should have security policies and procedures in place to combat such incidents, protect against potential insiders, and prevent unacceptable social media activities. 31% of German companies have formally defined ICT security policies [ENISA 2011b]. Integrating and enforcing social media security policies is easier when they can be implemented within a pre-existing ICT security framework. For instance, if the existing ICT security policies include monitoring and the organization wants to start legally monitoring social media, it might be able to do so as part of the existing monitoring.

As part of implementing this best practice, the CSG recommends including social engineering training along with security awareness training [Silowash 2012].

9% of Germans have security concerns related to performing activities via the internet [ENISA 2011b], which implies that the majority of Germans do not have security concerns about performing internet-based activities such as e-banking and purchasing goods. Approximately 5,000 phishing attacks occurred in Germany in 2010 [Fuerstenau 2010]. Germans' comfort with the internet and the increase of phishing attacks may be a problematic combination, making it more difficult for an organization to be vigilant about social media usage and making employees more susceptible to the attacks.

German is ranked 14th for individual usage of ICT [World Economic Forum 2012], which translates into a large number of people using social media and other internet components. If social media monitoring were legal in Germany, companies might need to invest substantial resources to do it, and, due to high cost and difficulty, it might have to be limited to searching for simple text phrases such as company or product names.

3.2.4.2 Effects of Germany's Laws

Germany has surrounding social media. During the application process, an employer can only ask for information specific to the job [Poerio 2012]. Therefore, employers may not be able to cast a wide net searching for information on social media [Poerio 2012]. Germany has drafted but not yet passed a law that is broader than many of the social media laws issued by some U.S. states and would prohibit the use of personal social network sites as part of the screening process (although sites like LinkedIn would not fall under this law) [Poerio 2012]. German employers may be able to monitor social media during employment but, "They must use third parties or obtain employee permission by, for example, 'becoming the employee's online "friend"'" [Poerio 2012]. Additionally, work councils may need to be informed of general monitoring policies [Proskauer 2012]. Finally, German employers have successfully used noncompete agreements with respect to social media [Poerio 2012].

3.2.4.3 Effects of Germany's Law Enforcement Profile

Policy, procedures, and training regarding social media use should be provided by organizations to all employees, contractors, and business partners. If social media use remains unmonitored or is left out of company training, it could allow for disclosure of company secrets and make people susceptible to social engineering attacks based on information that is disclosed both intentionally and unintentionally; therefore, a clear policy is necessary. The monitoring of social media, or personal data in general, varies across countries, as determined by law. Privacy is very important to Germans: 39% of them encrypt their internet traffic compared to only 18% of Americans [Federal Office for Information Security 2013d]. With the FDPA, Germany has stricter rules supporting data protection than many other countries [Federal Office for Information Security 2013d]. The BKA is tasked with monitoring the internet, including social media sites [bka.de 2013].

3.2.4.4 Effects of Germany's Corruption Profile

Social media postings that reveal a person's indiscretions or poor judgment could provide an avenue for exploitation or corruption through coercion. However, we found no significant indications that this kind of corruption exists in Germany.

3.2.4.5 Effects of Germany's Prevalent Culture and Subcultures

Because Germany is a low-context country [Hall 1976], organizations there should consider using direct and explicit statements when communicating social media policies and procedures. For example, Gustav Eirich, a German company, uses explicit low-context communication regarding social media policies: The company clearly states that all staff is forbidden from using Skype and discouraged from using Facebook [Hecking 2013]. Training materials can also benefit from having direct and explicit examples. To address the individualistic tendencies of German culture, an organization should consider including examples of the impact on individuals who violate social media policies and procedures. To increase compliance and institutionalization of social media policies and procedures, the organization should consider the organizational culture—and the various cultures represented in the workforce—when developing policies, procedures, and training materials.

3.2.5 Practice 9: Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.

For a summary of this best practice, see the appendix on page 63.

3.2.5.1 Effects of Germany's Technological Profile

The CSG recommends that organizations review their CSP's policies and practices to ensure it implements appropriate measures to protect the confidentiality, integrity, and availability of data [Silowash 2012]. Some German companies reduce their cloud-based risks related to confidentiality and integrity further by encrypting data hosted by CSPs, which adds an extra layer of security [Hecking 2013].

3.2.5.2 Effects of Germany's Laws

The Federal Commissioner for Data Protection and Freedom of Information created an orientation guide for cloud computing in 2011 [Working Groups 2011]. That guidance includes a reminder that the collection of personal information in the cloud is subject to the same data protection regulations, including the one that states the cloud user must ensure both organizational and technological measures are in compliance with these regulations [Working Groups 2011]. In addition, the guidance says that the cloud user must consider where the data processing may occur, with additional considerations present for data being transferred beyond Europe [Working Groups 2011]. Such considerations may include whether the nation's data protection framework has been deemed adequate or if the nation has negotiated a Safe Harbor Agreement, such as in the United States [export.gov 2013]. While rigorous requirements may be in place, one lawyer notes, "Enforcement is relatively lax" [O'Brien 2012].

3.2.5.3 Effects of Germany's Law Enforcement Profile

According to the CSG, organizations must work to establish that their CSP data protection and monitoring requirements for CSPs are consistent with the organization's own [Silowash 2012]. According to one Business Software Alliance report, Germany usually restricts criminal sanctions for serious cases that arise from using cloud computing, such as criminal conspiracy to interfere in the property rights of others [BSA 2012]. However, it is important to note that Germany, along with Japan and France, received a 10 out of 10 rating in the cybercrime section of that scorecard.

The report says, "Article 8 of the Telemedia Act expressly states that access providers are not legally responsible for their customers' content unless they collaborate with users in breaking the law" [BSA 2013a, p. 3]. It is not entirely clear which law enforcement agency or agencies would follow up on specific claims of malicious activity perpetrated by or through a CSP; however, the BSI wrote a paper called *Security Recommendations for Cloud Computing Providers* that serves to outline ways in which CSPs can meet at least the very minimum information security requirements [Federal Office for Information Security 2011].

3.2.5.4 Effects of Germany's Corruption Profile

As we discussed in Section 3.1.4, Germany was ranked 13th out of 176 in terms of perceived level of corruption, so corruption is not likely to be a significant negative factor when considering an effective implementation of this best practice. Low corruption (rated as better than in the United States) is a positive factor that makes implementing this best practice easier.

3.2.5.5 Effects of Germany's Prevalent Culture and Subcultures

Cloud services may be provided by organizations that reside in countries with cultures different than Germany's. To avoid any culturally based misunderstanding, an organization should consider the high-low context continuum, and various individualistic and collectivistic characteristics when developing its policies, practices, and training materials [Hofstede 2010, Hall 1976]. Security of data in the cloud is a high priority to organizations in Germany. Some German companies have added an extra layer of security by encrypting data hosted by CSPs [Hecking 2013].

Recent news regarding security of data hosted by U.S. CSPs has caused an increase in German organizations seeking additional measures to secure sensitive information from potential loss or unauthorized access [Hecking 2013, Abboud 2013]. This may potentially lead to the adoption of additional policies and practices that, when institutionalized, can influence an organization's culture to value and reinforce security. When selecting a provider, organizations may consider inquiring about its internal security policies and practices, and whether the CSP conducts audits or verifications to ensure that policies and practices are being performed accordingly.

3.3 Summary of Best Practice Implementation in Germany

In the tables below, we summarize our findings for Germany for all issues identified for all factors except laws and provide recommendations for effective cybersecurity practice implementations despite those issues.

Note: Because the CERT Division does not give legal advice, this table does not include legal issues and recommendations.

Cybersecurity Best Practice	Problems or Potential Problems for Implementing Best Practices	Recommendations
Germany – Technology		
CSG best practice 16	No specific issues demonstrated in this analysis	Ensure that core insider threat team members have secure methods to communicate with each other, in a physical location or via secure electronic communication. Ensure that insider threat teams understand who they need to coordinate with and report to. Be aware of the legality of such monitoring, which can be both a benefit and possible risk to the development of an insider threat program. Have policies and procedures that implement random audits of various data sources. Coordinate with the appropriate outside organizations to help insider threat teams prepare for handling incidents. Work with BSI and CERT-Bund so they know what to look for and can respond quickly to incidents when they occur.
CSG best practice 13	Email, logs, and data generated by the employee during the course of employment may be protected, and certain conditions may need to be met in order to review that information.	Be aware of the laws governing monitoring, especially if personally owned devices are used.
	Smartphones, which are becoming more commonplace, present a way for sensitive information to exit the organization using phone features such as email (personal or corporate), cameras, voice recording, and online storage.	Carefully control mobile phone usage in your organization and weigh the risks before allowing their use with corporate information systems. Build numerous levels of defense against a remote or off-site attack. Include mobile devices in your organization's risk assessments due to features on those devices that can be used to launch cyberattacks.

Cybersecurity Best Practice	Problems or Potential Problems for Implementing Best Practices	Recommendations
CSG best practice 4	No specific issues demonstrated in this analysis	Consider implementing additional monitoring capabilities to detect and prevent malicious insiders early on. Implement additional monitoring (within legal authority) during probationary periods or with positions that have high turnover rates. Review logs on a regular basis to detect and respond to possible malicious behavior. If your organization can't afford commercial products, implement open source solutions that involve lower overall costs.
CSG best practice 18	Social media opens employees to possible social engineering attacks. One such attack—phishing—has been on the rise and accounted for a loss of 17 million euros in 2010. Germany is ranked 14th for individual usage of Information and Communication Technologies (ICT), which translates into a large number of people using social media and other internet components. Approximately 5,000 phishing attacks occurred in Germany in 2010. Germans' comfort with the internet and the increase of phishing attacks may be a problematic combination, making it more difficult for an organization to be vigilant about social media usage and making employees more susceptible to the attacks.	Have security policies and procedures in place to combat social engineering attacks such as phishing, protect against potential insiders, and prevent unacceptable social media activities. If possible, legally monitor social media as part of your organization's existing monitoring. Include social engineering training along with security awareness training. If social media monitoring were legal in Germany, your organization might have to invest substantial resources to do it, and, due to high cost and difficulty, that monitoring might have to be limited to searching for simple text phrases such as company or product names.
CSG best practice 9	Some German companies reduce their cloud-based risks related to confidentiality and integrity further by encrypting data hosted by CSPs, which adds an extra layer of security.	Review your CSP's policies and practices to ensure it implements appropriate measures to protect the confidentiality, integrity, and availability of data. Implement encryption technology to protect data that is handled or processed by any third party, such as a CSP.

Cybersecurity Best Practice	Problems or Potential Problems for Implementing Best Practices	Recommendations
Germany - Prevalent Culture and Subcultures		
CSG best practice 16	Overall, Germany is homogeneous. However, it does have some small heterogeneous subcultures that might encompass people, groups, and possibly regions whose positioning may vary on the high-low context continuum, and individualistic and collectivistic scale.	When developing a formal insider threat program, consider the various cultural contexts in which your organization operates and the organization's culture, values, and beliefs. To increase the chance of a formal insider threat program being adopted and institutionalized, consider your organization's culture when developing the program. Consider using direct and explicit statements when developing policies, processes, and procedures associated with a formalized insider threat program. Consider the cultural composition of your organization's workforce when developing a formalized insider threat program. When developing guidelines and scenarios for your insider threat program, remember that companies operating in Germany usually focus on the good of the individual rather than the good of the group. Having that individualistic nature might increase the chances of employees reporting suspicious behavior. Communicate your organization's insider threat program in an explicit and direct way, and publicize the benefits the program will provide to employees.

Cybersecurity Best Practice	Problems or Potential Problems for Implementing Best Practices	Recommendations
CSG best practice 13	Because rules of privacy are important and observed, Germans were outraged when news of electronic surveillance operations was announced. German officials publicly cancelled the 1968-69 “spy” pact with the United States. Spiegel Online International has suggested a greater cooperation between German and U.S. intelligence agencies than has been publicly acknowledged. Regardless of whether it is true, the publicity that suggestion received could lead to a heightened awareness of an individual’s right to privacy. Employees may view monitoring and controlling remote access from all ends points, including mobile devices, as intruding on an employee’s personal rights and infringing on rules of privacy. The heightened awareness of monitoring in Germany, due to the recent alleged revelations from Edward Snowden in the news, could potentially impact employees’ loyalty and therefore their actions.	Consider publicizing the monitoring and controlling of remote access from all end points, including mobile devices, as a practice that is not only beneficial to the organization but also to each individual in it. Offer individual-level incentives that may influence the compliance, acceptance, behaviors, and actions associated with that monitoring and control.
CSG best practice 4	Lawmakers in the European parliament have suggested allowing cloud computing customers to opt out of their data being stored in the United States and to require supervision of the transfer of personal data to overseas CSPs.	Ensure that the effect on employees is minimal when performing background checks as part of the hiring process and periodic reinvestigations that follow organizational policies and privacy rules and laws. Ensure that all employees are informed of policies and practices associated with monitoring and responding to suspicious or disruptive behavior.
CSG best practice 18	No specific issues demonstrated in this analysis	Consider using direct and explicit statements when communicating social media policies and procedures. Use direct and explicit examples in training materials. Consider including examples of the impact on individuals who violate social media policies and procedures. To increase compliance and institutionalization of social media policies and procedures, consider the organizational culture—and the various cultures represented in the workforce—when developing policies, procedures, and training materials.

Cybersecurity Best Practice	Problems or Potential Problems for Implementing Best Practices	Recommendations
CSG best practice 9	Cloud services may be provided by organizations that reside in countries with cultures different than Germany's.	Consider the high-low context continuum, and various individualistic and collectivistic characteristics when developing your organization's policies, practices, and training materials.
	Security of data in the cloud is a high priority to organizations in Germany. Some German companies have added an extra layer of security by encrypting data hosted by CSPs.	When selecting a provider, consider inquiring about its internal security policies and practices, and whether the CSP conducts audits or verifications to ensure that policies and practices are being performed accordingly.
	Recent news regarding security of data hosted by U.S. CSPs has caused an increase in German organizations seeking additional measures to secure sensitive information from potential loss or unauthorized access. This may potentially lead to the adoption of additional policies and practices that, when institutionalized, can influence an organization's culture to value and reinforce security.	When selecting a provider, consider inquiring about its internal security policies and practices, and whether the CSP conducts audits or verifications to ensure that policies and practices are being performed accordingly.
Germany - Law Enforcement		
CSG best practice 16	Organizations may not have an established incident response plan or know which law enforcement agency to contact if an insider attack occurs.	Have specific criteria and thresholds for conducting inquiries, referring to investigators (who might include law enforcement), and requesting prosecution. Consult CERT-BUND and the National Cyber Security Committee before setting thresholds and criteria regarding cybersecurity-related policies. Implement an established incident response plan that aims to address any incidents that occur as a result of insider attacks. That plan should include information on how and when to contact cybersecurity law enforcement agencies.

Cybersecurity Best Practice	Problems or Potential Problems for Implementing Best Practices	Recommendations
CSG best practice 13	Mobile devices are ubiquitous in the country, and have features such as remote access, cameras, massive storage capabilities, and microphones that could be used for illegal data exfiltration. For instance, this might put the organization at risk of penalties if law enforcement organizations become aware of data exfiltration, particularly if the organization had not taken reasonable actions to protect it.	Consult resources from the National Cyber Security Committee and CERT-Bund, for help developing appropriate defenses against remote attacks.
	Germany has stringent data protection regulations, so organizations must be very careful to abide by those regulations.	Consult resources from the National Cyber Security Committee and CERT-Bund, for help developing appropriate defenses against remote attacks.
CSG best practice 4	Third parties may not be able to initiate important background checks regarding potential employees, depending on the law and its interpretation in a particular German state. A problem may exist for both the employer and the law enforcement agency providing the information, if there is a lack of clarity about relevant state laws, as well as how relevant laws (both federal and state) are interpreted in the particular state.	Organizations should consult with appropriate law enforcement agencies to determine what information the company may request on potential employees as well as which legal steps to take to gain it. Law enforcement agencies could provide support and critical information to private and public sector companies to ensure that they are provided with legal information regarding what steps they can take to secure their company by screening potential employees legally. This may help the organizations know if or how they are allowed to evaluate any previous criminal convictions, credit problems, or issues with past employment.

Cybersecurity Best Practice	Problems or Potential Problems for Implementing Best Practices	Recommendations
CSG best practice 18	The use of social networks is high in Germany and it ranks 14th out of 142 countries worldwide for individual usage [World Economic Forum 2012]. If social media use remains unmonitored or is left out of company training, it could allow for disclosure of company secrets and make people susceptible to social engineering attacks based on information that is disclosed both intentionally and unintentionally.	Provide the policy, procedures, and training on social media use to all employees, contractors, and business partners. Make sure the policy for social media use is written clearly.
	Privacy is important to Germans: 39% of them encrypt their internet traffic (compared to only 18% of Americans). This higher awareness and use of encryption can make it harder to prevent, detect, and respond to malicious insider activities. German organizations may find monitoring some insider activities difficult, due to encryption used by insiders. For example, organizations may miss detection of insider exfiltration of company intellectual property via an encrypted message.	None at this time
	With the FDPA, Germany has stricter rules supporting data protection than many other countries. Due to German privacy laws, German businesses and other non-governmental organizations may encounter difficulties in monitoring insider activities and IT communications. These organizations may also miss insider activities that may be occurring in order to exfiltrate data.	Consult resources from the National Cyber Security Committee and CERT-Bund for help developing appropriate defenses against insiders, while abiding by the FDPA.
CSG best practice 9	Germany usually restricts criminal sanctions for serious cases that arise from using cloud computing, such as criminal conspiracy to interfere in the property rights of others.	Since criminal sanctions will not apply in some cases, it is especially important to establish that your CSP's data protection and monitoring requirements, policies, and practices are consistent with your organization's data protection and monitoring requirements.
	It is not entirely clear which law enforcement agency or agencies would follow up on specific claims of malicious activity perpetrated by or through a CSP.	Consult resources from the National Cyber Security Committee and CERT-Bund for help determining which law enforcement agency or agencies should be contacted.

Cybersecurity Best Practice	Problems or Potential Problems for Implementing Best Practices	Recommendations
Germany - Corruption		
CSG best practice 16	Because Germany has a strong privacy and civil liberties view concerning workers' rights and privileges, employees might perceive an insider threat program negatively.	To help employees view insider threat programs in a more positive light, describe the formal insider threat program as • an example of German commitment to anti-corruption and order • supporting the private sector institution of the National Integrity System
CSG best practice 13	Although the software piracy rate in Germany was only 27% in 2010 (which is markedly lower than the EU's 33% average), the predominant sector involved in the piracy was German mid-level managers. Pirated software could introduce an unmanaged cybersecurity risk especially because it is often not eligible for software patches and bug fixes that can ameliorate known security vulnerabilities.	Implement frequent and widespread training and awareness to all employees on the dangers and risks of using pirated software, both on company assets and as an attack platform from employees' personal computers and devices. Consider providing incentives to employees who report pirated software that is discovered on company networks and implement sanctions on those employees that install the pirated software.
CSG best practice 4	No specific issues demonstrated in this analysis	None at this time
CSG best practice 18	Social media postings that reveal a person's indiscretions or poor judgment could provide an avenue for exploitation or corruption through coercion.	Train employees to avoid common social media mistakes that empower social engineering attacks and provide avenues for exploitation or coercion. Include the pitfalls that can arise from the use of social media by family members because they can also impact the employee.
CSG best practice 9	No specific issues demonstrated in this analysis	None at this time

4 Selected Comparisons: Findings for India and Germany

Table 2 through Table 6 below summarize some of the report's major findings, in a format for quick comparison between the countries, showing some major differences between the countries. The main body of this report contains much more of the regulatory, cultural, and technical information and analysis required to effectively implement practices in each nation.

Table 2: Summary of Report Findings: Information Related to Laws

Laws	**India**	**Germany**
Cyber laws	IT Act of 2011 [MCIT 2008]; Not a Signatory of the Budapest Convention on Cybercrime [Council of Europe 2001]	Implementation of the Budapest Convention on Cybercrime
Privacy laws	IT Rules [Reporters Without Borders 2012, MCIT 2011, Linklaters 2011a, Linklaters 2011b, Hunton & Williams 2011c] (some exceptions may apply)	Federal Personal Data Protection Act of 2001 [German Federal States 2010]; Act on Employee Data Protection; Federal Data Protection Act [McAfee 2013, Federal Office for Information Security 2013e]
Human Resources (HR) Laws	Persons with Disabilities Act [Medindia 1995]; Industrial Law [Bhasin 2007]; Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act [Gopalakrishnan 2013]	Federal General Equal Treatment Act [Gibson Dunn 2006]; Other Labor Laws [Corley 2011, Berkowitz 2013, Allen 2013]

Table 3: Summary of Report Findings: Information Related to Culture

Cultural Concern	India	Germany
Homogeneous versus heterogeneous	Heterogeneous with strong regional affiliations; high cultural diversity at the national level	Heterogeneous with regional affiliations; low cultural diversity at the national level
Linguistic diversity [Ethnologue 2013]	High; 18 national languages; 454 living languages	Low; 1 national language; 27 living languages
Communication [Hall 1976]	High-context; implicit cultural knowledge; variations on high-low context scale assumed	Low-context; explicit cultural knowledge; variations on high-low context scale assumed
Individualistic versus collectivistic [Hofstede 2010]	Collectivistic; good of the group valued over good of the individual; rules of individual privacy not as important	Individualistic; good of the individual valued over good of the group; rules of individual privacy important
Perception of time [Hall 1976]	Polychronic; time is fluid, flexible, and adjusted to meet the needs of the people; tardiness tolerated	Monochronic; time is structured and compartmentalized; time is perceived as having the potential of being wasted; promptness emphasized

Table 4: Summary of Report Recommendations with Respect to Cultural Concerns

Cultural Concern	India	Germany
Homogeneous versus heterogeneous	Understanding the internal and external cultural diversity and influences would be beneficial when developing a program.	Understanding the internal and external cultural diversity and influences would be beneficial when developing a program.
Linguistic diversity	High diversity; should be considered when developing policy, processes, procedures, and training	Low diversity; should not be a strong issue except with non-native German speakers
Communication	The implicit aspect of communication should be included in training materials, examples, and modes of communication. In-person training would be beneficial.	Policies, processes, procedures, and training materials need to be explicit and direct. Both online training and in-person training should be used.
Individualistic versus collectivistic	Emphasize the benefits to the group and the individual of reporting suspicious behavior; training materials should include examples that stress benefits to the larger group, society, etc.	Emphasize benefits to individuals of reporting suspicious behaviors and repercussions for violators. The importance of an individual's right to privacy can be an issue.
Perception of time	Reporting suspicious behavior in a timely and understandable way should be stressed; training materials should include examples of what is timely. Less adherence to schedules would not necessarily indicate an issue.	To increase the identification of suspicious behavior, capitalize on structured and compartmentalized perceptions of time to separate "normal" work hours and routine from what is outside the norm.

Table 5: Summary of Report Findings: Information Related to Law Enforcement

Law Enforcement Concern	India	Germany
Active enforcement	Indications of minimal involvement in cybersecurity enforcement [Zargar 2013]	Indications of active involvement in cybersecurity enforcement [ENISA 2011b]
Cyber capability	Indications of minimal cyber techniques and forensic capabilities [MCIT 2013]	Indications of advanced cyber techniques [ENISA 2011a] and forensic capabilities
Constraints	Significant limitations imposed by the Information Technology Act of 2000 as amended in 2008 [Zargar 2013]	Restrictions on data collection due to significant privacy and civil liberties concerns [Miller 2010]
Interactions	Rarely called upon for help with cybercrime (Many companies prefer outside consultants or cyber forensic response companies.[7])	Appear actively involved in helping companies that are victims of cybersecurity crimes [von Hein 2011]

Table 6: Summary of Report Findings: Information Related to Corruption

Corruption Concern	India	Germany
External perception	Scored 36 on Corruption Perceptions Index [Transparency International 2012] (94th out of 176); high corruption	Scored 79 on Corruption Perceptions Index [Transparency International 2012] (13th out of 176); low corruption
Internal perception	54% of households paid bribes for basic government services [Transparency International 2013b]; software piracy rampant [Rangaswamy 2007]	70% of population believes that corruption has increased/will increase [Transparency International 2013a]; software piracy among mid-level management [Nill 2010]
Effects of corruption factor on best practice implementation	May help bolster need for insider threat programs, as well as all other CSG best practices	May help insider threat programs best practices if framed in right light, little impact to other CSG best practices
Unknown impacts	Could corruption hide failure to adhere to cybersecurity, or could corruption hide draconian cybersecurity measures?	Could corruption of workforce representatives and software piracy hurt cybersecurity?

Notable qualities of IT in India and Germany are shown in Figure 1 and Figure 2 below.

India has a developing IT system with a low internet access rate and a 3G maximum bandwidth (except for a handful of cities with 4G service). Although cellphone access has significantly increased recently, smartphone access is currently not widespread, due to cost. Law enforcement with respect to cybersecurity has notable problems. We discussed cultural findings that could help with effective communication and implementation of CSG-recommended controls; however, due to India's wide variety of subcultures, more analysis is recommended for specific locations, organizations, and other conditions. Corruption as measured by the CPI is relatively high compared

[7] Source: interview with employee working in Indian cybersecurity industry. Interviewee and company names withheld.

to Germany or the United States, which poses difficulties with effectively implementing some of the CSG-recommended controls in support of the best practices.

India has unique IT factors, some of which may allow a malicious insider to attack:

- weak encryption
  - Government requires encryption keys to be no stronger than 40 bits.
    - Longer encryption keys must be stored with the government.
- National Technical Research Organisation [sic] (NTRO)
  - is similar to NSA [Unnithan 2007]
  - has attempted to crack Google and Skype Servers
  - compromised several India-based servers (email, news, etc.)
- monitors all communications
  - central monitoring system
- statistics
  - Mobile internet traffic is 59.36% of internet traffic in India.
  - The internet has an 11% penetration rate.
  - 2.4% of the population have > 4Mbps connections.

Figure 1: Notable Highlights of IT in India

Germany has a modern IT system with high bandwidth; a high internet and mobile connection access rate; a low corruption rate as measured by the CPI; a relatively high number of cybersecurity regulations; relatively thorough public awareness of cybersecurity issues; and a high percentage of companies using structured, information security management systems. Often, implementing the CSG-recommended controls in Germany did not appear to require many changes. However, laws limiting monitoring or affecting the way background checks are performed may change the potential implementation of CSG-recommended controls. In the body of this report, we discussed cultural findings that could help with effective communication and implementation of CSG-recommended controls.

These notable percentages apply to Germany's IT:

- 82% of German households have access to the internet.
- 9% of the German population limit their internet activities due to security concerns.
- 72% of the German population use IT security software to protect private systems and data.
- 31% of German enterprises have a formally defined, ICT security policy.
- Germany is set to reach internet access speeds of 50MB for 75% of households by 2015 and 100% by 2018.

Figure 2: Notable Highlights of IT in Germany

5 Conclusions and Future Work

This framework-based analysis of applying insider threat best practices in an international context revealed important considerations for organizations that have non-U.S. business partners, outsourcing, offshoring, and supply chains. We found that some of the controls recommended in the U.S.-focused CSG would support best practices more effectively if modified or publicized differently for insider threat programs in (and covering) India or Germany. Additionally, we found some issues impeding effective implementation of some best practices, without yet finding an effective solution for them. By including India, with its large population, this report has nominally analyzed the implementation of insider threat best practices for 17% of the world's current population. However, because India is culturally diverse and has a low internet access rate, much more analysis can be done. This is an initial, exploratory effort that is not exhaustive. On some subjects, the resources used for this initial effort provided more data and analysis for one country than the other. Additionally, new revelations about the countries and factors discussed in this report have appeared in the news during the writing of this report [Poitras 2013, Spiegel 2013b, Larson 2013]; however, due to time limits, only some of those revelations could be considered here.

We plan to analyze additional countries using this framework and to create some new controls. For some of the controls recommended by the CSG, we identified implementation problems for Germany or India, but we were unable to find the needed, substitution controls. Future work should include deeper, more detailed data and analytical insights about each factor, drawn from a variety of subject matter experts and additional reference documents. Future work will incorporate more information from recent revelations that appeared in the news during the writing of this report, which affects analyses of technological systems [Poitras 2013, Spiegel 2013d, Larson 2013]. Those revelations will also impact the profile of each country's laws, law enforcement, and culture, which in turn will affect our framework-based analysis of implementation of best practices for mitigating insider threats in India, Germany, and beyond.

Appendix Summary of CSG Best Practices Analyzed

The CSG best practice summaries below are excerpted from the 2012 Third Worldwide Cybersecurity Summit conference paper titled "Best Practices Against Insider Threats in All Nations" [Flynn 2012].

Practice 4: Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.

Organizations should conduct background checks and periodic reinvestigations on prospective employees, contractors, and workers from trusted business partners to identify insiders' personal, professional, and financial stressors. The content of the background check varies according to local, current laws, but it may include checks for previous criminal convictions, verification of credentials and past employment, a credit check, and competence evaluations from past employers. Organizations should identify risk levels for all positions and more thoroughly investigate individuals applying for or occupying higher risk positions. Organizations must consistently enforce sanctions for all rule violators or risk emboldening insiders. Responses to behavioral disruptions include a warning; punitive action; or referral to an Employee Assistance Program (EAP), which might reduce the risk of an insider deciding to harm the organization.

Practice 9: Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.

An organization must ensure its data protection and monitoring requirements for cloud providers are commensurate with the organization's own requirements. Protections include physical and technological requirements, as well as human resources practices for cloud provider employees. Cloud providers should perform pre-hire background checks that are regularly updated after hire, obtain acknowledgement of policies and practices, and provide training on these topics. One potential risk in the cloud environment is the rogue administrator, including hosting company administrators, virtual image administrators, system administrators, and application administrators. These insiders may exploit vulnerabilities in the cloud or use the cloud as an attack platform. Organizations must review the cloud provider's SLA and insurance to ensure that risks and liability are suitably addressed. They must also review the policies and practices of their provider to ensure it is implementing appropriate measures to protect the confidentiality, integrity, and availability of data. The SLA might include the ability to audit the provider, or requirements specific to human resources supply chain management or security breach notification. The organization, a third party, or the provider itself should continuously monitor the distributed infrastructure, review audit logs, aggregate diagnostic data, and periodically audit the cloud infrastructure to ensure virtual machines and other cloud systems meet security configuration requirements.

Practice 13: Monitor and control remote access from all end points, including mobile devices.

The increasing trend toward a mobile workforce has also increased the potential for malicious use of mobile devices. Their cameras, microphones, mass storage, and communications capabilities could be used to capture and exfiltrate sensitive information. Organizations must be aware of potential risks posed by mobile application functionality that insiders could use maliciously. A multi-layered defense can include prohibiting personally owned devices, limiting remote access to critical data, limiting the number of privileged users with remote access, and using application gateways for non-organizational equipment. Organizations should more closely log and audit all remote transactions and ensure that remote access is disabled during employee termination.

Practice 16: Develop a formalized insider threat program.

An insider threat program should be enterprise-wide and establish clearly defined roles and responsibilities for preventing, detecting, and responding to insider incidents. The goal of an insider threat program is to develop clear criteria for identifying insider threats, a consistent procedure for implementing technical and nontechnical controls to prevent malicious insider behavior, and a response plan in the event an insider does harm the organization.

Legal counsel is vital during the information-gathering process to ensure all evidence is gathered and maintained in accordance with legal standards and to issue a prompt legal response when necessary. Legal counsel should also ensure that information is shared properly among the insider threat team members, for instance, to ensure the lawful privacy of employees' mental and physical health information.

Practice 18: Be especially vigilant regarding social media.

Organizations should provide training as well as policies and procedures about social media. Such outlets may allow employees to share organizational information that adversaries could use to target current or former employees, either as victims or co-conspirators. For example, attackers might use organizational information to refine spear phishing attempts or fraud schemes. Companies should consider potentially problematic postings on social media, both intentional and unintentional, and should consider developing a social media policy in accordance with applicable laws and regulations.

References

URLs are valid as of the publication date of this document.

[Abboud 2013]
Abboud, Leila & Sandle, Paul. “Analysis: European Cloud Computing Firms See Silver Lining in PRISM Scandal.” *Reuters* (June 17, 2013). http://www.reuters.com/article/2013/06/17/us-cloud-europe-spying-analysis-idUSBRE95G0FK20130617

[Aguilar 2007]
Aguilar, M. *Finally: German Whistleblowing Guidelines Released* (2007). http://www.edwardswildman.com/files/Publication/876dc86e-0111-47e9-b532-cbd053145b74/Presentation/PublicationAttachment/51060d8e-a3b4-4b08-b7a2-332f0026df2a/Finally_German%20Whistleblowers%20GuidlinesReleased_pdf.pdf

[Ahmad 2009]
Ahmad, Nehaluddin. “Restrictions on Cryptography in India- A Case Study of Encryption and Privacy.” *Computer Law and Security Review 25*, 2 (2009): 173-180.

[Akamai 2013]
Akamai Technologies. *State of the Internet* (2013). http://www.akamai.com/stateoftheinternet/?gclid=CK6v_4O9-7kCFaNxOgodF3YAtQ

[Allen 2013]
Allen, Keith. *Labor Laws in Germany.* http://www.ehow.com/list_6750376_labor-laws-germany.html (2013).

[AP 2013]
Associated Press. “German prosecutors charge Lebanese-German man with spying for Syria on exiled dissidents.” *Fox News* (July 22, 2013). http://www.foxnews.com/world/2013/07/22/german-prosecutors-charge-lebanese-german-man-with-spying-for-syria-on-exiled/

[Arnold 2012]
Arnold, Ulli; Neubauer, Joerg; & Schoenherr, Tobias. “Explicating Factors for Companies' Inclination Towards Corruption in Operations and Supply Chain Management: An Exploratory Study in Germany.” *International Journal of Production Economics, 138*, 1 (July 2012): 136-147. Elsevier B.V.

[Bafna 2012]
Bafna, Sanjay. “India has 7,36,654 Mobile Towers and Only 96,112 BTS’s are 3G Enabled!” *TelecomTalk.info* (December 21, 2012). http://telecomtalk.info/india-has-736654mobile-towers-and-only-96112bts-are-3g-enabled/103422/

[Bafna 2013]
Bafna, Sanjay. "Airtel Acquires 100 Percent Stake in Qualcomm Founded WBSPL – 4G Spectrum Holder in Mumbai, Delhi, Kerala and Haryana." *TelecomTalk.info* (October 18, 2013). http://telecomtalk.info/airtel-acquires-100-percent-stake-in-qualcomm-founded-wbspl-4g-spectrum-holder-in-mumbai-delhi-kerala-and-haryana/109856/

[BBC 2011]
BBC Monitoring International Reports. *German Government Responds to Parliamentary Inquiry into Cyber Security Strategy* (November 14, 2011). Academic OneFile. http://go.galegroup.com/ps/i.do?id=GALE%7CA272657995&v=2.1&u=cmu_main&it=r&p=AONE&sw=w&asid=72fef38f6d373be448359a9079fceaa0

[BBC 2013]
BBC. "Germany Ends Spy Pact with US and UK After Snowden." *BBC News Europe* (August 2, 2013). http://www.bbc.co.uk/news/world-europe-23553837

[Berkowitz 2013]
Berkowitz, Alan; Johnson, Thomas; Thomas, Phillippe; Wynn-Evans, Charles. "Recent Employment Law Developments in Germany." *International Employment Law Review: August 2013*, Issue 4. http://www.jdsupra.com/legalnews/international-employment-law-review-aug-07382/ (August 12, 2013).

[Bernstein 2004]
Bernstein, Eckhard. *Culture and Customs of Germany*. Greenwood, 2004.

[Betts 2010]
Betts, Paul. *Within Walls: Private Life in the German Democratic Republic*. Oxford University Press, 2010.

[Bhasin 2007]
Bhasin, Lalit. "India: Labour and Employment Laws of India." http://www.mondaq.com/india/x/50440/employee+rights+labour+relations/Labour+And+Employment+Laws+Of+India (August 24, 2007).

[Bitkom 2013]
Bitkom. *App-Usage and Mobile Enterprise in Germany* (February 3, 2013). http://www.messefrankfurt.com/content/corporate/frankfurt/en/media/entertainmentmediacreation/m-days/aktuelles/_jcr_content/mainParsys/downloadbox_0/downloadboxParsys/download_9/file.res/BITKOM+Hand-out+M-Days+04+02+2013+-+englisch.pdf

[bka.de 2013]
Bundeskriminalamt (Germany). *Internet Crime* (2013). http://www.bka.de/nn_194550/EN/SubjectsAZ/InternetCrime/internetCrime__node.html?__nnn=true

[blackhat.com 2013]
Blackhat Europe 2013. https://www.blackhat.com/eu-13/

[Borchers 2013]
Borchers, D. *German Federal Criminal Police Acquires Interim Government Trojan from Gamma* (January 17, 2013). http://www.h-online.com/security/news/item/German-Federal-Criminal-Police-acquires-interim-government-trojan-from-Gamma-1786026.html

[Bowe 2012]
Bowe, Rebecca. *Growing Mistrust of India's Biometric ID Scheme." Electronic Frontier Foundation* (May 4, 2012). https://www.eff.org/deeplinks/2012/05/growing-mistrust-india-biometric-id-scheme

[Boyer 2000]
Boyer, Dominic C. "On the Sedimentation and Accreditation of Social Knowledges of Differences: Mass Media, Journalism, and the Reproduction of East/West Alterities in Unified Germany." *Cultural Anthropology 15*, 4 (2000): 459-491.

[BSA 2012]
Business Software Alliance. *BSA Global Cloud Computing Scorecard: Germany* (2012). http://cloudscorecard.bsa.org/2012/assets/PDFs/country_reports/Country_Report_Germany.pdf

[BSA 2013a]
Business Software Alliance. *BSA Global Cloud Computing Scorecard: Germany* (2013). http://cloudscorecard.bsa.org/2013/assets/PDFs/country_reports/Country_Report_Germany.pdf

[BSA 2013b]
Business Software Alliance. *Competitive Advantage, The Economic Impact of Properly Licensed Software* (2013). http://portal.bsa.org/insead/assets/studies/2013softwarevaluestudy_en.pdf.

[CCC 2013]
Chaos Computer Club (2013). http://www.ccc.de/en/

[CCIC 2013]
Crime Branch, Criminal Investigation Department, Mumbai Police, Mumbai, India. *Cyber Crime Investigation Cell* (2013). http://cybercellmumbai.gov.in/

[Center for Strategic and International Studies 2011]
Center for Strategic and International Studies. *Cybersecurity and Cyberwarfare* (2011). www.unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf

[cert.org 2013]
cert.org. *CERT Information Security Classes* (2013). http://www.cert.org/training/

[CIA 2013a]
Central Intelligence Agency. *The World Factbook* (2013). https://www.cia.gov/library/publications/the-world-factbook/

[CIA 2013b]
Central Intelligence Agency. *The World Fact Book Europe: Germany* (2013). https://www.cia.gov/library/publications/the-world-factbook/geos/gm.html

[CIA 2013c]
Central Intelligence Agency. *The World Fact Book: India* (2013). https://www.cia.gov/library/publications/the-world-factbook/geos/in.html

[City Mayors Foundation 2012]
City Mayors Foundation. *Largest Indian Cities* (2012). http://www.citymayors.com/gratis/indian_cities.html

[CNET 1997]
CNET News. *40-Bit Crypto Proves No Problem* (January 31, 1997). http://news.cnet.com/2100-1017-266268.html

[COE 2004]
Council of Europe. *Convention on Cybercrime, CETS No.: 185* (July 1, 2004). http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG

[COE 2009]
Council of Europe. *Cybercrime Legislation-Country Profile: Germany* (2009). http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/countryprofiles/cyber_cp_Germany_2010_July_EN.pdf

[COE 2013]
Council of Europe. *Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems* (2003-2013). http://conventions.coe.int/Treaty/Commun/print/ChercheSig.asp?NT=189&CL=ENG

[Collins 2010]
Collins, P.; Stein, L.: & Trombino, C. "Consider the Source: How Weak Whistleblower Protection Outside the United States Threatens to Reduce the Impact of the Dodd-Frank Reward Among Foreign Nationals." *The Third Annual National Institute on the Foreign Corrupt Practices Act,* October 21, 2010. http://www.perkinscoie.com/files/upload/10_25Article.pdf

[Connors 2013]
Connors, Will. "RIM Launches Q5 BlackBerry for Developing World." *Wall Street Journal* (2013). http://online.wsj.com/article/SB10001424127887323893504578557430527664470.html

[Constantin 2009]
Constantin, L. *German Cyber-Cops Close Down Hacking Forum* (March 5, 2009). http://news.softpedia.com/news/German-Cyber-cops-Close-Down-Hacking-Forum-106063.shtml

[Corley 2011]
Corley, Terry. *Germany – Country Background Screening Essentials.* http://internationalscreening.wordpress.com/tag/the-federal-data-protection-act-bundesdatenschutzgesetz-bdsg/ (June 12, 2011).

[Council of Europe 2001]
Council of Europe. *Convention on Cybercrime*. http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm (November 23, 2001).

[Croft 2011]
Croft, W. *Germany rolls-out LTE to rural areas* (June 2, 2011). https://gsmaintelligence.com/analysis/2011/06/germany-rolls-out-lte-to-rural-areas/283/

[Deutsche Bank Research 2011]
Deutsche Bank Research. *Update on Online and Mobile Banking.* Deutsche Bank Research, November 2011.

[DHS 2012a]
U.S. Department of Homeland Security National Cyber Security Division (NCSD), Critical Infrastructure Protection - Cyber Security (CIP CS). *2012 Cybersecurity Forecast* (2012).

[DHS 2012b]
U.S. Department of Homeland Security Office of Inspector General. *Transportation Security Administration Has Taken Steps To Address the Insider Threat But Challenges Remain* (September 25, 2012). http://www.oig.dhs.gov/assets/Mgmt/2012/OIGr_12-120_Sep12.pdf

[DOD 2011]
United States Department of Defense. *Department of Defense Strategy for Operating in Cyberspace* (July 2011). http://www.defense.gov/news/d20110714cyber.pdf

[DOD 2012]
Department of Defense. *Defense Science Board Task Force Report: The Role of Autonomy in DoD Systems* (July 2012). http://www.dtic.mil/docs/citations/ADA566864

[DOJ 2009]
United States Department of Justice, Civil Rights Division. *Information and Technical Assistance on the Americans with Disabilities Act* (2009). http://www.ada.gov/

[DOS 2013]
United States Department of State. *Joint Statement on U.S.-Germany Cyber Bilateral Meeting* (June 14, 2013). http://www.state.gov/r/pa/prs/ps/2013/06/210677.htm

[Dougherty 2008]
Dougherty, Sean. “Labour Regulation and Employment Dynamics at the State Level in India.” *OECD Economics Department Working Papers 624*. OECD Publishing, 2008. http://dx.doi.org/10.1787/241014565862

[DSCI 2013]
Data Security Council of India. *About Us* (2013). http://www.dsci.in/about-us

[Dutta 2012]
Dutta, S. & Bilbao-Osorio, B. "The Global Information Technology Report 2012." *World Economic Forum* (2012). http://www3.weforum.org/docs/Global_IT_Report_2012.pdf

[Dwucet 2012]
Dwucet, Michael. *Team Presentation: CERT Bund, Federal Office for Information Security (BSI)*. Federal Office for Information Security, 37th TF-CSIRT meeting, September 27, 2012. http://www.terena.org/activities/tf-csirt/meeting37/dwucet-cert-bund.pdf

[EEOC 2012]
United States Equal Employment Opportunity Commission. *EEOC Enforcement Guidance: Consideration of Arrest and Conviction Records in Employment Decisions Under Title VII of the Civil Rights Act of 1964* (April 25, 2012). http://www.darkreading.com/vulnerability/another-researcher-hit-with-threat-of-ge/229402356

[ENISA 2011a]
ENISA. *Cybersecurity Strategy for Germany* (2011). http://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy-2011-1

[ENISA 2011b]
ENISA. *Germany Country Report* (May 2011). http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Germany.pdf

[Ethnologue 2013]
Ethnologue.com. *Summary by Country* (2013). http://www.ethnologue.com/statistics/country

[European Commission 2012]
European Commission. *Data retention: Commission Takes Germany to Court Requesting That Fines Be Imposed* (May 31, 2012). http://europa.eu/rapid/press-release_IP-12-530_en.htm

[export.gov 2013]
export.gov. *Welcome to the U.S.-EU & U.S.-Swiss Safe Harbor Frameworks* (2013). http://export.gov/safeharbor/

[Federal Commissioner for Data Protection and Freedom of Information 2013]
The Federal Commissioner for Data Protection and Freedom of Information (Germany). *The Use of the Internet and E-mail at the Workplace* (2013). http://www.bfdi.bund.de/EN/Topics/labour/Artikel/InternetEMailsAtWorkplace.html?nn=410268

[Federal Ministry of Economics and Technology 2010]
Federal Ministry of Economics and Technology (Germany). *ICT Strategy of the German Federal Government: Digital Germany 2015* (November 2010). http://www.bmwi.de/English/Redaktion/Pdf/ict-strategy-digital-germany-2015,property=pdf,bereich=bmwi2012,sprache=en,rwb=true.pdf

[Federal Ministry of the Interior 2008]
Federal Ministry of the Interior (Germany). *Protecting Critical Infrastructures—Risk and Crisis Management* (2008). http://www.bmi.bund.de/SharedDocs/Downloads/EN/Broschueren/Leitfaden_Schutz_kritischer_Infrastrukturen_en.pdf?__blob=publicationFile

[Federal Office for Information Security 2011]
Federal Office for Information Security (Germany). *Security Recommendations for Cloud Computing Providers* (June 22, 2011).

[Federal Office for Information Security 2013a]
Federal Office for Information Security (Germany). *CERT-Bund* (2013). https://www.bsi.bund.de/CERT-Bund_en

[Federal Office for Information Security 2013b]
Federal Office for Information Security (Germany). *History* (2013). https://www.bsi.bund.de/EN/TheBSI/History/history_node.html

[Federal Office for Information Security 2013c]
Federal Office for Information Security (Germany). *Task and Objectives of the IT Situation Centre* (2013). https://www.bsi.bund.de/EN/Topics/IT-Crisis-Management/IT-Situation-Centre/itsituationcentre_node.html

[Federal Office for Information Security 2013d]
Federal Office for Information Security (Germany). *Layer Universally Applicable Aspects - B 1.5 Data Privacy Protection; IT Grundschutz Catalogues: New* (2013). https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BaustDatenschutz/moduleb01005_pdf.pdf?__blob=publicationFile

[Federal Office for Information Security 2013e]
Federal Office for Information Security (Germany). *Data Protection Acts.* http://www.bfdi.bund.de/cln_134/EN/DataProtectionActs/DataProtectionActs_node.html (2013).

[Ferran 2013]
Ferran, L. “New Snowden Documents Show NSA-Germany Spy Links: Report.” *ABC News* (July 22, 2013). http://abcnews.go.com/blogs/headlines/2013/07/new-snowden-documents-show-nsa-germany-spy-links-report/

[Flynn 2012]
Flynn, L; Huth, C.; Trzeciak, R.; & Buttles-Valdez, P. “Best Practices Against Insider Threats for All Nations.” *Proceedings of the Third Worldwide Cybersecurity Summit*, New Delhi, India, Oct. 30-31, 2012. EWI and IEEE. Forthcoming. http://cybersummit2012.com/content/selected-papers

[Fuerstenau 2010]
Fuerstenau, M. & Farivar, C. “Cybercrime in Germany on the Rise.” *Deutsch Welle* (September 7, 2010). http://dw.de/p/P66X

[Fuerstenau 2013]
Fuerstenau, M. “Both Criminals and Police Are Using the Internet.” *Deutsch Welle* (February 21, 2013). http://www.dw.de/both-criminals-and-police-are-using-the-internet/a-16616770

[Gabrielson 2008]
Gabrielson, Bruce; Goertzel, Karen; Hoenicke, B.; Kleiner, D.; & Winograd, T. "The Insider Threat to Information Systems: A State-of-the-Art Report." *Contract SPO700-98-D-4002*. Herndon, VA: Information Assurance Technology Analysis Center (IATAC), 2008.

[Gallagher 2012]
Gallagher, Ryan. *Does Germany’s Plan to Create Its Own Spyware Violate Its Constitution?* (September 7, 2012). http://www.slate.com/blogs/future_tense/2012/09/07/chaos_computer_club_german_agency_bka_hiring_developers_to_create_spyware_.html

[Garyali 2013]
Garyali, N. “Top 16 GSM and CDMA Dual-SIM Phones in India for September 2013.” *Know Your Mobile India* (September 29, 2013). http://www.knowyourmobile.in/android/6903/top-16-gsm-and-cdma-dual-sim-phones-india-september-2013

[Gaudin 2007]
Gaudin, Sharon. “German Police Arrest 10 International Phishing Suspects.” *Information Week* (September 13, 2007). http://www.informationweek.com/german-police-arrest-10-international-ph/201806309

[German Federal Ministry of Justice 2013]
German Federal Ministry of Justice. *The Digital World* (2013). http://www.bmj.de/EN/Subjects/DigitalRights/_node.html

[German Federal States 2010]
German Federal States. *German Bundesdatenschutzgesetz (BDSG), a Federal Data Protection Act* (2010). http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile

[Gibson Dunn 2006]
Gibson Dunn. *German Parliament Passes General Equal Treatment Act, Which Will Have a Considerable Impact on German Employment Practice*. http://www.gibsondunn.com/publications/pages/GermanParliamentPassesGeneralEqualTreatmentActWhichWillHaveaConsiderableImpactonGermanEmployment.aspx (July 20, 2006).

[GO-gulf.com 2013]
GO-gulf.com (blog). http://www.go-gulf.com/blog/cyber-crime/

[Goel 2012]
Goel, Asheesh. *International Anti-Bribery and Corruption Trends and Developments.* Ropes & Gray, 2012. http://www.ropesgray.com/asheeshgoel/~/media/Files/articles/2012/05/20120521_ABC_Book.ashx

[Gopalakrishnan 2013]
Gopalakrishnan, Veena; Solanki, Ajay Singh; & Shroff Vikram. “India’s New Labour Law - Prevention of Sexual Harassment at the Workplace.” http://www.mondaq.com/india/x/238076/Discrimination+Disability+Sexual+Harassment/Indias+New+Labour+Law+Prevention+Of+Sexual+Harassment+At+The+Workplace (May 9, 2013).

[Government of India 1950]
Government of India. *Constitution of India* (1950). http://www.wipo.int/wipolex/en/details.jsp?id=6771

[Gowda 2011]
Gowda, Sadananda & Bhavan, Raj. “Justice Sodhi Frontrunner for Lokayukta.” *The Times of India.* http://articles.timesofindia.indiatimes.com/2011-09-21/bangalore/30183948_1_resignation-n-k-sodhi-governor (September 21, 2011).

[Guess 2004]
Guess, C. Dominik. “Decision Making in Individualistic and Collectivistic Cultures. *Online Readings in Psychology and Culture 4*, 1 (2004). http://dx.doi.org/10.9707/2307-0919.1032

[Hall 1976]
Hall, Edward T. *Beyond Culture*. Anchor Books, 1976.

[Hecking 2013]
Hecking, Claus. “Snooping Fears: German Firms Race to Shield Secrets.” *Spiegel Online International* (July 23, 2013). http://www.spiegel.de/international/germany/german-firms-fear-industrial-espionage-after-snowden-leaks-a-912624.html

[Heng 2012]
Heng, Stefan. *Cloud Computing: Clear Skies Ahead*. Deutsche Bank, March 1, 2012.

[Heylman 2012]
Heylman, Susan R. “Germany Finds Anonymous Job Applications Benefit Women, Older, Workers, Immigrants.” *Society for Human Resource Management* (May 23, 2012).

[Hickok 2011]
Hickok, Elonnai. *Encryption Standards and Practices* (April 5, 2011). http://cis-india.org/internet-governance/blog/privacy/privacy_encryption

[Higgins 2011]
Higgins, K.J. *Another Researcher Hit with Threat of German Anti-Hacking Law* (April 27, 2011). http://www.darkreading.com/vulnerability/another-researcher-hit-with-threat-of-ge/229402356

[Hindu Business Line 2011]
Hindu Business Line. “Corruption in India Has Become Worse.” *Hindu Business Line* (August 24, 2011). http://www.thehindubusinessline.com/industry-and-economy/corruption-in-india-has-become-worse-ratan-tata/article2392208.ece

[Hindu Business Line 2012]
Hindu Business Line. "Majority of Indian Employees Approve Personal Use of Social Media at Work." *Hindu Business Line* (June 13, 2012). http://www.thehindubusinessline.com/industry-and-economy/info-tech/majority-of-indian-employees-approve-personal-use-of-social-media-at-work/article3523591.ece

[Hofstede 2010]
Hofstede, G. and Minkov, N. *Culture and Organizations: Software of the Mind,* 3rd ed. McGraw-Hill, 2010.

[Hübner 2013]
Hübner, Alexander. "Germany Arrests Two Dutch Citizens in Cyber Bank Heist." *Chicago Tribune* (May 10, 2013). http://articles.chicagotribune.com/2013-05-10/business/sns-rt-us-usa-crime-cybercrimebre9480pz-20130509_1_u-s-justice-department-cash-machines-two-middle-eastern-banks

[Hunton & Williams 2011a]
Hunton & Williams, LLP. "German DPAs Publish Comprehensive FAQs on Statutory Data Breach Notification Requirement." *Privacy and Information Security Law Blog* (May 30, 2011). http://www.huntonprivacyblog.com/2011/05/articles/german-dpas-publish-comprehensive-faqs-on-statutory-data-breach-notification-requirement/

[Hunton & Williams 2011b]
Hunton & Williams, LLP. "Outsourcers Exempt from India's Privacy Regulations." *Privacy and Information Security Law Blog* (August 24, 2011). http://www.huntonprivacyblog.com/2011/08/articles/outsourcers-exempt-from-indias-privacy-regulations/

[Hunton & Williams 2011c]
Hunton & Williams, LLP. "India Drafts New Privacy Regulations." *Privacy and Information Security Law Blog* (May 18, 2011). https://www.huntonprivacyblog.com/2011/05/articles/india-drafts-new-privacy-regulations/

[Hunton & Williams 2012]
Hunton & Williams, LLP. "German Authorities Publish Traffic Data Retention Guide for Telecoms." *Privacy and Information Security Law Blog* (October 3, 2012). http://www.huntonprivacyblog.com/2012/10/articles/german-authorities-publish-traffic-data-retention-guide-for-telecoms/

[Hunton & Williams 2013a]
Hunton & Williams, LLP. "German Federal Office for Information Security Issues Guidance on Consumerization and BYOD." *Privacy and Information Security Law Blog* (February 7, 2013). http://www.huntonprivacyblog.com/2013/02/articles/german-federal-office-for-information-security-issues-guidance-on-consumerization-and-byod/

[Hunton & Williams 2013b]
Hunton & Williams, LLP. "German Ministry Publishes Draft Law for Cybersecurity Breach Notification." *Privacy and Information Security Law Blog* (March 15, 2013). http://www.huntonprivacyblog.com/2013/03/articles/german-ministry-publishes-draft-law-for-cybersecurity-breach-notification/

[IIBF 2005]
Indian Institute of Banking and Finance. "Cyber Laws in India." Legal Aspects Of Banking Operations. Macmillan India, 2005. http://www.iibf.org.in/documents/Cyber-Laws-chapter-in-Legal-Aspects-Book.pdf

[India Biz News 2012]
India Biz News. "GSM Market Update." *India Biz News* (February 10, 2012). http://www.indiabiznews.com/?q=node/2381

[Indian Parliament 2008]
Indian Parliament. *The Information Technology Act of 2000 (No. 21 of 2000), amended in 2008* (2008). http://cactusblog.files.wordpress.com/2010/01/it_act_2008.pdf

[InformationWeek 2013]
InformationWeek. *Indian Enterprises BYOD Incorporation in a Favorable Light, Reveals Dell Survey* (June 12, 2013). http://www.informationweek.in/mobile/13-06-12/indian_enterprises_see_byod_incorporation_in_a_favorable_light_reveals_dell_survey.aspx

[IPTU 2011]
India Pakistan Trade Unit. *Employment Law in India* (October 2011). http://www.iptu.co.uk/content/india_employment_law.asp

[ISEA 2013]
Information Security Education & Awareness, Department of Electronics and Information Technology (DeitY) - Ministry of Communications and Information Technology, Government of India. *Cyber Crime Cells (in India)* (August 2013). http://infosecawareness.in/cyber-crime-cells-in-india

[ITU 2012a]
International Telecommunications Union. *Mobile Data Accounts for 10% of Worldwide Internet Usage* (June 22, 2012). http://www.itu.int/ITU-D/ict/newslog/Mobile+Data+Accounts+For+10+Of+Worldwide+Internet+Usage.aspx

[ITU 2012b]
International Telecommunications Union. *Understanding Cybercrime: Phenomena, Challenges and Legal Response* (September 2012).

[izmf.de 2013]
izmf.de. *The Development of Digital Mobile Communications in Germany* (2013). http://www.izmf.de/en/content/development-digital-mobile-communications-germany

[Jain 2003]
Jain, R. B. & Bawa, P. S. *National Integrity System Transparency International Country Study Report, India 2003.* Transparency International, 2003. www.transparency.org/content/download/1652/8377/file/india.pdf

[Karandikar 2012]
Karandikar, Abhay. "India Needs Umbrella Body on Telecom Standards to Foster Creation of IPR and Develop Indigenous Products." *Economic Times* (August 16, 2012). http://articles.economictimes.indiatimes.com/2012-08-16/news/33232949_1_telecom-equipment-indian-ipr-telecom-market

[Karganis 2013]
Karganis, J. & Renrema, L. *Copy Culture in the US and Germany*. The American Assembly, 2013. http://americanassembly.org/sites/americanassembly.org/files/download/project/copy-culture.pdf

[Kelly-Holmes 2002]
Kelly-Holmes, Helen. "German Language: Whose Language, Whose Culture?" *Contemporary German Culture Studies.* Ed. Alison Phipps. London: Arnold, 2002.

[Kerala.com 2013]
Kerala.com. *Kerala at a Glance* (2013). http://www.kerala.com/about_kerala/about_kerala.php

[Kington 2013]
Kington, T. "Across Europe, Nations Mold Cyber Defenses." *DefenseNews*(July 9, 2013). http://www.defensenews.com/article/20130709/DEFREG01/307090008/Across-Europe-Nations-Mold-Cyber-Defenses

[Knigge 2013]
Knigge, Michael. "German Jitters Over Cyber Attacks." *Deutsche Welle* (August 3, 2013). http://www.dw.de/german-jitters-over-cyber-attacks/a-16658040

[KPMG 2010]
KPMG International. *India Fraud Survey* (2010). http://www.kpmg.com/IN/en/IssuesAndInsights/ThoughtLeadership/KPMG_Fraud_Survey_2010.pdf

[KPMG 2011]
KPMG International. *KPMG Unveils Survey on Bribery and Corruption* (2011). http://www.kpmg.com/IN/en/Press%20Release/Press_Release_Bribery_Corruption_Survey.pdf

[KPMG 2012]
KPMG International. *India Fraud Survey* (2012). http://www.businessworld.in/c/document_library/get_file?uuid=3f13daf0-c87d-4050-af99-ef18ff5925c8&groupId=520986

[Krell 2013]
Krell, Eric. “Forecast for Global Background Checks: HR Professionals Say the Outlook Remains Foggy.” *HR Magazine 58*, 4 (April 1, 2013). http://www.shrm.org/Publications/hrmagazine/EditorialContent/2013/0413/Pages/0413-international-background-screening.aspx

[Krishna 2013]
Krishna, R. Jai. "Q&A: BlackBerry Bets on Competitive India Market." *Wall Street Journal Tech Blog* (July 19, 2013). http://blogs.wsj.com/digits/2013/07/19/qa-blackberry-bets-on-competitive-india-market/

[Kumar 2011]
Kumar, A. *Essay on Prohibition of Discrimination on Certain Grounds as per Indian Constitution* (November 12, 2011). http://www.preservearticles.com/2011111216873/essay-on-prohibition-of-discrimination-on-certain-grounds-as-per-indian-constitution.html

[Kumar 2012]
Kumar, M. *India Ties Up with US for Cyber Security* (September 13, 2012). http://www.dnaindia.com/india/1740178/report-india-ties-up-with-us-for-cyber-security

[Kumar 2013a]
Kumar, Aditya. “Chequered Pasts: The Failure of Technical Education and a Glut of IT Graduates Are Fuelling Résumé Fraud and a Burgeoning Background Verification Industry.” *Caravan Magazine* (April 1, 2013). http://caravanmagazine.in/reportage/chequered-pasts

[Kumar 2013b]
Kumar, Hari. “Unique ID Program Introduces Instant Verification Services.” http://india.blogs.nytimes.com/2013/05/24/aadhar-program-introduces-instant-verification-services/?_r=0 (May 24, 2013).

[LaDosa 2006]
LaDosa, Chaise. “The Discursive Malleability of an Identity: A Dialogic Approach to Language ‘Medium’ Schooling in North India.” *Journal of Linguistic Anthropology, 16*, 1 (2006): 36–57.

[Landler 2008]
Landler, Mark. “Volkswagen Corruption Trial Includes Seamy Testimony.” *New York Times* (Jan. 16, 2008). http://www.nytimes.com/2008/01/16/business/16bribe.html.

[Larson 2013]
Larson, Jeff; Perlroth, Nicole; & Shane, Scott. “Revealed: The NSA’s Secret Campaign to Crack, Undermine Internet Security.” *ProPublica* (September 5, 2013). http://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption

[LawTeacher 2013]
LawTeacher. “Many Reasons Like Lower Value of Indian Currency. *Lawteacher.net* (2013) http://www.lawteacher.net/constitutional-law/essays/many-reasons-like-lower-value-of-indian-currency-constitutional-law-essay.php#ixzz2iTg9aYVf

[Lerner 2012]
Lerner, Carolyn (Special Counsel, U.S Office of Special Counsel). *Memorandum: Agency Monitoring Policies and Confidential Whistleblower Disclosures to the Office of Special Counsel and to Inspectors General* (June 20, 2012). http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/omb_and_osc_memos_on_agency_monitoring_policies.pdf

[Levin 2012]
Levin, Avner; Goodrick, Paul; & Ilkina, Daria. *Securing Cyberspace: A Comparative Review of Strategies Worldwide* (2012). http://www.ryerson.ca/content/dam/tedrogersschool/privacy/documents/Ryerson_cyber_crime_final_report.pdf

[Linklaters 2011a]
Linklaters. *India – Welcome Clarification on Sensitive Personal Data Rules.* http://www.linklaters.com/Publications/Publication1403Newsletter/TMT-newsletter-September-2011/Pages/India-data-security-laws.aspx (September 20, 2011).

[Linklaters 2011b]
Linklaters. *India – New Data Security Laws and Rules for Sensitive Personal Information.* http://www.linklaters.com/Publications/Publication1403Newsletter/TMT_Newsletter_May_2011/Pages/India_New_Data_Security_Laws_Rules_Sensitive_Personal_Information.aspx (May 27, 2011).

[Lüders 2013]
Lüders, Christine. *Welcome to the Federal Anti-Discrimination Agency!* (2013). http://www.antidiskriminierungsstelle.de/EN/Home/home_node.html

[Mathur 2012]
Mathur, Nayanika. “Transparent-Making Documents and the Crisis of Implementation: A Rural Employment Law and Development Bureaucracy in India.” *PoLAR: Political and Legal Anthropology Review 35*, 2 (2012): 167–185.

[Maughan 2009]
Maughan, Douglas. "A Roadmap for Cybersecurity Research." *U.S. Department of Homeland Security* (November 2009). http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf

[Mazzarella 2010]
Mazzarella, William. “Beautiful Balloon: The Digital Divide and the Charisma of New Media in India.” *American Ethnologist 37,* 4 (2010): 783-804.

[McAfee 2013]
McAfee. *Germany*. http://www.mcafee.com/us/regulations/europe/germany.aspx (2013).

[MCIT 2008]
Department of Electronics and Information Technology (DeitY) - Ministry of Communications and Information Technology, Government of India. *Information Technology Act.* http://deity.gov.in/content/information-technology-act (2008).

[MCIT 2011]
Department of Electronics and Information Technology (DeitY) - Ministry of Communications and Information Technology, Government of India. *Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules* (April 11, 2011). http://deity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf

[MCIT 2013]
Department of Electronics and Information Technology (DeitY) - Ministry of Communications and Information Technology, Government of India. *Cyber Crime Cells in India.* http://infosecawareness.in/cyber-crime-cells-in-india (November 22, 2013).

[Medindia 1995]
Medindia. *Persons with Disabilities Act 1995*. http://www.medindia.net/indian_health_act/persons-with-disabilities-act-1995-preliminary.htm (1995).

[Meeker 2012]
Meeker, Mary and Wu, Liang. *Internet Trends @ Stanford – Bases* (December 3, 2012). http://www.kpcb.com/insights/2012-internet-trends-update

[Mehta 2013]
Mehta, S. "India's Speech Impediments." *New York Times* (February 5, 2013). http://www.nytimes.com/2013/02/06/opinion/indias-limited-freedom-of-speech.html

[Miller 2010]
Miller, Russell A. *Balancing Security and Liberty in Germany.* http://jnslp.com/wp-content/uploads/2010/12/04_Miller_vol4no2.pdf (2010).

[Mitchell 2009]
Mitchell, Lisa Nayanika. *Language, Emotion, and Politics in South India: The Making of a Mother Tongue*. Indiana University Press, 2009.

[Mobile Indian 2013]
The Mobile Indian. *Helps You Choose* (2013). http://www.themobileindian.com/handset-guide/category-search/GSM%2BCDMA

[Mudde 2007]
Mudde, R. *Area and Population (Karnataka)* (July 14, 2007). http://www.karnataka.com/profile/area/

[Muthukumaran 2008]
Muthukumaran, B. "Cyber Crime Scenario in India." *Criminal Investigations Department Review* (January 2008): 17-23. http://www.gcl.in/downloads/bm_cybercrime.pdf

[Naavi.org 2013]
Naavi.org. *Cyber Crime Police Stations in Different States of India* (2013). http://www.naavi.org/cl_editorial_04/cyber_Crime_ps.htm

[NASSCOM 2013]
NASSCOM. *Vision and Mission* (2013). http://www.nasscom.in/vision-and-mission

[NCC Group 2011]
NCC Group. *Cyber Prosecution - A Sign Of Things To Come?* (June 20, 2011). http://www.nccgroup.com/de/nachrichten/news/2011/jun/cyber-prosecution-a-sign-of-thing-to-come/

[NCRB 2012]
National Crime Records Bureau (Ministry of Home Affairs) (India). *Crime in India 2012* (2012). http://ncrb.gov.in/.

[Nill 2010]
Nill, Alexander; Schibrowsky, John; & Peltier, James W. "Factors That Influence Software Piracy: A View from Germany." *Communications of the ACM 53*, 6 (June 2010): 131-134.

[Noack 2010]
Noack, Torsten & Kubicek, Herbert."The Introduction of Online Authentication as Part of the New Electronic National Identity Card in Germany." *Identity in the Information Society 3*, 1 (July 2010): 87-110. Springer Netherlands.

[NSTC 2011]
Executive Office of the President, National Science and Technology Council. *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program* (December 2011). http://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf

[O'Brien 2012]
O'Brien, Kevin. " New European Guidelines to Address Cloud Computing." *New York Times* (July 1, 2012). http://www.nytimes.com/2012/07/02/technology/new-eu-guidelines-to-address-cloud-computing.html?pagewanted=all&_r=0

[OSC 2012]
U.S. Office of Special Counsel. *Agency Monitoring Policies and Confidential Whistleblower Disclosures to the Office of Special Consel and to Inspectors General*. http://www.osc.gov/documents/press/2012/press/Agency%20Monitoring%20Policies%20and%20Confidential%20Whistleblower%20Disclosures%20to%20the%20Office%20of%20Special%20Counsel%20and%20Inspectors%20General.pdf (June 20, 2012).

[Paczkowski 2013]
Paczkowski, John. *BlackBerry Targets India with Launch of Mid-Range Q5* (July 17, 2013). http://allthingsd.com/20130717/blackberry-targets-india-with-launch-of-mid-range-q5/

[Pandharipande 2002]
Pandharipande, R. "Minority Matters: Issues in Minority Languages in India." *International Journal on Multicultural Societies 4*, 2 (2002). http://www.unesco.org/most/vl4n2pandhari.pdf

[Poerio 2012]
Poerio, J.M. & Bain, L.E. “Social Media in the Workplace: Employer Protection Versus Employee Privacy.” *ABA International Law News 41*, 4 (Fall 2012).

[Poitras 2012]
Poitras, Laura; Rosenbach, Marcel; and Holger Stark. “Codename ‘Apalachee’: How America Spies on Europe and the UN,” *Spiegel Online International* (August 26, 2013). http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html

[Ponemon 2012a]
Ponemon Institute. *2012 Cost of Cyber Crime Study: United States* (2012). http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf

[Ponemon 2012b]
Ponemon Institute. *2012 Cost of Cyber Crime Study: Germany* (2012).

[Prakash 2013]
Prakash, P. "Indian Surveillance Laws & Practices Far Worse Than US." *The Economic Times* (June 13, 2013). http://articles.economictimes.indiatimes.com/2013-06-13/news/39952596_1_nsa-india-us-homeland-security-dialogue-national-security-letters

[Prashad 2013]
Prashad, Vijay. "India’s Cowardly Display of Servility." *The Hindu* (July 3, 2013). http://www.thehindu.com/opinion/op-ed/indias-cowardly-display-of-servility/article4874219.ece

[Privacy International 2012]
Privacy International. “Chapter III: Surveillance Policies.” *Report: India* (2012). https://www.privacyinternational.org/reports/india/iii-surveillance-policies(2012)

[Proskauer 2012]
Proskauer. *Social Media in the Workplace Around the World 2.0* (2012). http://www.proskauer.com/files/uploads/Documents/2012_ILG_Social_Network_Survey_Results_Social_Media_2.0.pdf

[Rana 2010]
Rana, Shayne. “Intex 5030 Triple SIM (GSM + GSM + CDMA) Handset.” *tech2* (March 8, 2010). http://tech2.in.com/reviews/mobile-phones/intex-5030-triple-sim-gsm-gsm-cdma-handset/112872

[Rangaswamy 2007]
Rangaswamy, Nimmi. *Regulating India's Digital Public Cultures: A Grey or Differently Regulated Area.* Springer Verlag, July 2007.

[Rao 2008]
Rao, P. “Human Resource Practice in India.” *Society for Human Resource Management* (2012). http://www.shrm.org/Education/hreducation/Documents/Rao%20India%20HR%20Practices%20To%20Post.ppt

[Rapp 2012]
Rapp, R.; Gady, F.; Parmar, S.; & Rauscher, K. "India's Critical Role in the Resilience of the Global Undersea Communications Cable Infrastructure." *Strategic Analysis 36*, 3 (2012). http://www.tandfonline.com/doi/abs/10.1080/09700161.2012.670444

[Reporters Without Borders 2012]
Reporters Without Borders *Internet Enemies Report 2012*. http://march12.rsf.org/i/Report_EnemiesoftheInternet_2012.pdf (March 12, 2012).

[Resource Centre for Cyber Forensics 2013]
Resource Centre for Cyber Forensics (2013). http://www.cyberforensics.in

[Reuters 2008]
Reuters. “German Court Permits Limited Cybermonitoring.” *New York Times* (February 28, 2008). http://www.nytimes.com/2008/02/28/world/europe/28germany.html

[Roberts 2008]
Roberts, Bill. *Protecting Employee Data Globally* (May 1, 2008). http://www.shrm.org/Publications/hrmagazine/EditorialContent/Pages/5HR%20Tech-Managing%20Global%20HR%20Data%20Privacy%20Issues.aspx

[Routley 2013]
Routley. *India Compliance Guidelines to Cloud Services* (April 30, 2013). http://www.symantec.com/connect/articles/india-compliance-guidelines-cloud-services

[Roy 2013]
Roy, Prasanto K. *Snowden, Surveillance and Snooping in India: FAQs* (July 7, 2013). http://www.sify.com/news/snowden-surveillance-and-snooping-in-india-faqs-news-international-nhhmOgfcbhj.html

[Ryan 2011]
Ryan, Patrick S.; Merchant, Ronak; & Falvey, Sarah. “Regulation of the Cloud in India.” *Journal of Internet Law 15*, 4 (October 2011). http://ssrn.com/abstract=1941494

[Saxena 2013]
Saxena, Anupam. *50 Percent Smartphone Users in India Don't Have an Active Data Connection, Android Leads: Survey* (February 8, 2013). http://gadgets.ndtv.com/mobiles/news/50-percent-smartphone-users-in-india-dont-have-an-active-data-connection-android-leads-survey-328151

[Scally 2013]
Scally, Derek. “Pressure Builds in Germany over Edward Snowden Claims.” *Irish Times* (July 11, 2013). http://www.irishtimes.com/news/world/europe/pressure-builds-in-germany-over-edward-snowden-claims-1.1459597

[Schönbohm 2011]
Schönbohm, Arne. *Germany Must Defend Against Cyber Attacks*. http://archive.atlantic-community.org/index/articles/view/Germany_Must_Defend_Against_Cyber_Attacks_ (2011)

[Security B-Sides 2013]
Security B-Sides Wiki (2013). http://www.securitybsides.com/w/page/12194156/FrontPage

[Sharma 2011]
Sharma, Nagendar. "Lokayukta: Anti-Corruption Watchdog." http://www.hindustantimes.com/Lokayukta-anti-corruption-watchdog/Article1-738662.aspx. August 27, 2011.

[Sharma 2012a]
Sharma, A. & Bahree, M. "In India, Dreaming of A 4G World." *Wall Street Journal* (July 25, 2012). http://online.wsj.com/news/articles/SB10000872396390443295404577547002264600084

[Sharma 2012b]
Sharma, P. *Transparency for the Inclusive Governance, An Assessment of India*. World Economic Forum, 2012. http://www.weforum.org/reports/transparency-inclusive-governance-assessment-india

[Shaw 2011]
Shaw, T. *Information Security and Privacy, A Practical Guide for Global Executives, Lawyers and Technologists*. ABA Publishing, 2011.

[Shenoy 2013]
Shenoy, Deepti. "Courting Substantive Equality: Employment Discrimination Law in India." *University of Pennsylvania Journal of International Law 34*, 3 (2013): 611-640. https://www.law.upenn.edu/live/files/2256-shenoy34upajintll6112013pdf

[Shinde 2009]
Shinde, Ranjit. "GSM, CDMA Players Maintain Subscriber Growth Momentum." *Economic Times* (March 18, 2009). http://articles.economictimes.indiatimes.com/2009-03-18/news/28465507_1_subscriber-cdma-players-rcom

[Shroff 2012]
Shroff, Vikram & Sinha, Neha. *Background Checks in India* (2012). http://www.shrm.org/LegalIssues/EmploymentLawAreas/Documents/LRReport0112.pdf

[Silowash 2012]
Silowash, George; Cappelli, Dawn; Moore, Andrew; Trzeciak, Randall; Shimeall, Timothy; & Flynn, Lori. *Common Sense Guide to Mitigating Insider Threats*, 4th Edition (CMU/SEI-2012-TR-012). Software Engineering Institute, Carnegie Mellon University, 2012. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=34017

[Singh 2012]
Singh, S. *Smartphone Market Share Trends by Country: Android Dominant, iPhone Gains, Windows Phone Slips Further* (December 25, 2012). http://www.tech-thoughts.net/2012/12/smartphone-market-share-trends-by-country.html

[Singh 2013]
Singh, Talwant. *Cyber Law and Information Technology* (updated 2013). http://www.indlii.org/CyberLaw.aspx

[SN 2013a]
SN, Vikas. *Akamai Report: India Ranks 74th In Broadband Adoption; 16.2M Unique IPs* (2013). http://www.medianama.com/2013/07/223-akamai-internet-report-q1-2013/

[SN 2013b]
SN, Vikas. *Apple Q3-FY13: 31.2M iPhones & 14.6M iPads Sold; iPhone Sales In India Up 400%* (2013). http://www.medianama.com/2013/07/223-apple-q3-fy13-earnings/

[Spiegel 2013a]
Spiegel. "Indispensible Exchange: Germany Cooperates Closely with NSA." *Spiegel Online* (July 8, 2013). http://www.spiegel.de/international/world/spiegel-reveals-cooperation-between-nsa-and-german-bnd-a-909954.html

[Spiegel 2013b]
Spiegel. "Merkel Speaks: Chancellor Defends Intelligence Monitoring." *Spiegel Online* (July 10, 2013). http://www.spiegel.de/international/germany/german-chancellor-merkel-defends-work-of-intelligence-agencies-a-910491.html

[Spiegel 2013c]
Spiegel. "Key Partners: Secret Links Between Germany and the NSA." *Spiegel Online* (July 22, 2013). http://www.spiegel.de/international/world/german-intelligence-worked-closely-with-nsa-on-data-surveillance-a-912355.html

[Spiegel 2013d]
Spiegel. "Privacy Scandal: NSA Can Spy on Smart Phone Data." *Spiegel Online* (September 7, 2013). http://www.spiegel.de/international/world/privacy-scandal-nsa-can-spy-on-smart-phone-data-a-920971.html

[Srivastava 2013]
Srivastava, Samar. "Why Whistle Blowing Is So Hard in India." *Forbes India* (May 17, 2013). http://forbesindia.com/blog/business-strategy/why-whistle-blowing-is-so-hard-in-india/

[Stanton 2006]
Stanton, Jeffrey M. & Stam, Kathryn R. *The Visible Employee: Using Workplace Monitoring and Surveillance to Protect Information Assets-Without Compromising Employee Privacy or Trust.* Information Today, 2006.

[statewatch 2013]
statewatch.org. “German Police Instructed Tunisia and Egypt on Internet Surveillance Prior to Revolutions.” *statewatch.org* (May 22, 2013). http://www.statewatch.org/news/2013/may/08ger-north-africa-surveillance.html

[Stern 2013]
Stern, S. “Indian Media Reports Progress on Undersea Cable Repairs.” *East-West Institute* (January 3, 2013). http://www.ewi.info/indian-media-reports-progress-undersea-cable-repairs

[Strack 2011]
Strack, Guido. “Whistleblowing in Germany.” *Whistleblowing in Defense of Proper Action. Praxiology: The International Annual of Practical Philosophy and Methodology 18* (2011). Transaction Publishers, New Brunswick, NJ. http://www.whistleblower-net.de/pdf/WB_in_Germany.pdf

[Symantec 2013]
Symantec. *India Sees 280 Percent Increase in Bot Infections - Symantec Internet Security Threat Report 18* (April 29, 2013).
http://www.symantec.com/en/in/about/news/release/article.jsp?prid=20130428_01

[The German Way 2013]
The German Way. *Cell Phones in Europe* (2013). http://www.german-way.com/travel-and-tourism/telephone-tips-for-germany/cell-phones-in-europe/

[Thomas 2011]
Thomas, D. “Nokia Boosted by Sales of Cheap Handsets.” *Financial Times* (October 20, 2011).
http://www.ft.com/cms/s/0/11bbf530-fb11-11e0-bebe-00144feab49a.html#axzz2iTfi2IOH

[Thomas 2013]
Thomas, T. “Show Cause Notice Keeps Undersea Cable Ship Off India Coast.” *Hindu Business Line* (January 1, 2013). http://www.thehindubusinessline.com/industry-and-economy/info-tech/show-cause-notice-keeps-undersea-cable-ship-off-india-coast/article4262423.ece

[Times of India 2012]
Times of India. “Airtel launches 4G in Kolkata.” *Times of India* (April 11, 2012).
http://timesofindia.indiatimes.com/business/india-business/Airtel-launches-4G-in-Kolkata/articleshow/12617622.cms

[TRAI 2013]
Telecom Regulatory Authority of India. *The Indian Telecom Services Performance Indicators: October - December, 2012* (2013).
http://www.trai.gov.in/WriteReadData/PIRReport/Documents/Indicator%20Reports%20-%20Dec-12.pdf

[Transparency International 2012]
Transparency International. Corruption Perceptions Index (2012).
http://cpi.transparency.org/cpi2012/results/

[Transparency International 2013a]
Transparency International. *Global Corruption Barometer* (2013). http://www.transparency.org/research/gcb/overview

[Transparency International 2013b]
Transparency International. *India: Speaking up for Integrity* (2013). http://www.transparency.org/news/feature/india_speaking_up_for_integrity

[Transparency International 2013c]
Transparency International. *National Integrity System Germany, Short Version* (2013). http://www.transparency.org/whatwedo/pub/national_integrity_system_germany_short_version

[Travis 2013]
Travis, A. “European Commission Backs Merkel's Call for Tougher Data Protection Laws.” *The Guardian* (July 15, 2013). http://www.theguardian.com/world/2013/jul/15/european-commission-angela-merkel-data-protection?CMP=twt_gu

[UIDAI 2013]
UIDAI. Unique Identification Authority of India homepage. http://uidai.gov.in/ (2013).

[UNCTAD 2012]
United Nations Conference on Trade and Development. *World Investment Prospects Survey 2010 – 2012* (2012). unctad.org/en/pages/PublicationArchive.aspx?publicationid=620

[Unnithan 2007]
Unnithan, Sandeep. “Spy versus spy.” http://indiatoday.intoday.in/content_mail.php?option=com_content&name=print&id=1067 (September 7, 2007).

[USC 2013]
United States Code - Section 1030. *Fraud and Related Activity in Connection with Computers* (2013). http://codes.lp.findlaw.com/uscode/18/I/47/1030

[Varshney 2013]
Varshney, R. “Koramangala Firms Keep Background Check on Staff.” *Economic Times* (January 21, 2013). http://articles.economictimes.indiatimes.com/2013-01-21/news/36462889_1_verification-employee-fraud-koramangala

[von Hein 2011]
von Hein, Matthias & Impey, Joanna. http://www.dw.de/germanys-cyber-defense-center-goes-fully-online/a-15161387 (June 16, 2011).

[Wang 2011]
Wang, Chun-Lin. "How to Regulate Computer Crime in Germany Criminal Law." *6th International Conference on Computer Science & Education (ICCSE 2011)*. Singapore, August 3-5, 2011. IEEE. Piscataway, NJ. 384-385.

[Working Groups 2011]
Working Groups on Technology and Media of the Conference of Federal and State Data Protection Commissioners. *Cloud Computing: An Orientation Guide, v1.0* (September 26, 2011). http://www.bfdi.bund.de/EN/Topics/technologicalDataProtection/Artikel/OHCloudComputing.pdf?__blob=publicationFile

[World Economic Forum 2012]
World Economic Forum. *The Global Information Technology Report 2012: Living in a Hyper-connected World*. http://www3.weforum.org/docs/Global_IT_Report_2012.pdf (2012).

[World Economic Forum 2013]
World Economic Forum. *The Global Information Technology Report 2013 Data Platform* (2013). http://www.weforum.org/issues/global-information-technology/gitr-platform

[World Time Zone 2013]
World Time Zone. *GSM World Coverage Map and GSM Country List* (2013). http://www.worldtimezone.com/gsm.html

[York 2013]
York, Jillian C. "NSA Leaks Prompt Surveillance Dialogue in India." *Electronic Frontier Foundation (EFF)* (July 10, 2013). https://www.eff.org/deeplinks/2013/07/nsa-leaks-prompt-surveillance-dialogue-india

[Zargar 2013]
Zargar, Haris. *India's Information Technology Act has not been effective in checking cybercrime: Expert* (2013). http://www.dnaindia.com/scitech/1818328/report-india-s-information-technology-act-has-not-been-effective-in-checking-cyber-crime-expertReferences/Bibliography
URLs are valid as of the publication date of this document.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	April 2014	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
International Implementation of Best Practices for Mitigating Insider Threat: Analyses for India and Germany	FA8721-05-C-0003

6. AUTHOR(S)

Lori Flynn, Carly Huth, Palma Buttles-Valdez, Michael Theis, George Silowash, Tracy Cassidy, Travis Wright, Randy Trzeciak

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2014-TR-008

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFLCMC/PZE/Hanscom Enterprise Acquisition Division 20 Schilling Circle Building 1305 Hanscom AFB, MA 01731-2116	

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

This report analyzes insider threat mitigation in India and Germany, using the new framework for international cybersecurity analysis described in the paper titled "Best Practices Against Insider Threats in All Nations," applying the framework to specific countries for the first time. Using that framework, cybersecurity standards are considered with respect to analysis that takes into account a country's technologies, relevant laws, law enforcement, corruption, and prevalent culture and subcultures. This report provides a detailed profile for each of these factors for each country and considers five best practices for mitigating insider threats recommended in the *Common Sense Guide to Mitigating Insider Threats*.

This report is intended to help organizations implement cybersecurity best practices internationally. In part, this analysis is meant to help readers understand challenges in India and Germany, plus mitigations for the challenges that are particularly useful in those countries. These insights can be used by organizations that outsource to, offshore to, or have supply chains that include these countries. Furthermore, this report's findings may be helpful on a wide scale for implementing general cybersecurity best practices in countries that share similarities with India or Germany, with regard to the factors studied. Technical, physical, and administrative controls that are helpful for implementing best practices in India and Germany may be helpful for similar countries. Likewise, particular controls may be ineffective (and require substitution controls) in similar countries. This is an initial, exploratory effort that is not exhaustive.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Insider Threat, Best Practices, India, Germany, International, Analysis, Mitigation, Controls, Implementation, InformationTechnology, Law, Law Enforcement, Culture, Subculture, Corruption	103

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL